HACKER JOURNAL

Anno 2 - N. 20
27 Febbraio / 13 Marzo 2003

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Contributors: Bismark.it, , CAT4R4TTA, DaMe`, Nicola D'Agostino, lele-Altos.tk, Roberto "decOder" Enea, Paola Tigrino, witch_blade.

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

C'È CHI DICE NO

Diciamocelo, gli smanettoni di tutto il mondo hanno un incubo ricorrente che li fa rabbrividire. Non si tratta di un virus micidiale, di un'intrusione a livello root nel proprio computer, e nemmeno di immensi database coi dati personali di ogni navigatore, custoditi nei sotterranei di qualche agenzia governativa o di un monopolista del software a scelta. L'incubo è molto più concreto, vicino e familiare. E, almeno ogni tanto, si realizza.

Sto parlando delle richieste di aiuto da parte di parenti, amici e conoscenti:

- "Visto che sei così bravo col computer, perché non vieni a dare un'occhiata al mio che non funziona bene"?

- "Hum... ma che cos'ha?"

- "Non funziona bene"

Nel mio caso, l'incubo si è materializzato la settimana scorsa. Il portatile di mio cognato era diventato lento fino all'inverosimile. D'accordo, aveva un processore a 500 MHz e 64 Mbyte di RAM; una macchina ormai vecchiotta. Da qui a impiegare trenta secondi per aprire una qualsiasi finestra, e tre minuti per lanciare Outlook, ce ne passa.

Constatato che non sembravano esserci errori di configurazione, stavo pensando di attuare il classico piano B (reinstallazione di Windows, Me in quel caso), quando ho cominciato a guardare con sospetto la dozzina di icone sparse tra scrivania e barra delle applicazioni. Un paio di acceleratori di download, qualche visualizzatore di notizie, scimmiette colorate da far rimbalzare sullo schermo. Oltre a ciò, c'era l'intero pacchetto di utility del Dottore Imbalsamato (quello che da 20 anni ha la stessa faccia sulle sue scatole...).

Prima di passare alla reinstallazione, ho quindi provato a scaricare AdAware, che ha subito individuato 4 diversi Spyware, collegati a una decina di programmi. Zappato via il tutto, il sistema ha cominciato a essere quasi usabile. Poi sono passato a sfoltire l'installazione di Norton SystemWorks (capito chi era il Dottore?); ho lasciato l'antivirus e LiveUpDate, da attivarsi manualmente, e ho sostituito il firewall con ZoneAlarm. Risultato? Pur non essendosi trasformato in una scheggia, il computer è tornato pienamente utilizzabile.



Due riflessioni: quasi sempre le utility miracolose, tipo "ti moltiplico la velocità di download", altro non fanno che rallentare il sistema, e producono effetto contrario. Statene alla larga.

La seconda riflessione è che, quando si vuole acquistare un qualsiasi software, spesso il produttore cerca in ogni modo di farci installare almeno una mezza dozzina dei suoi prodotti. Certo, si possano personalizzare le installazioni, ma la maggior parte degli utenti non sa proprio come fare. Qual è la soluzione? Diffidare di tutto ciò che si installa nel proprio computer; analizzarlo con attenzione, leggere tutti i documenti, spulciare ogni opzioni. Prendere davvero il controllo della propria macchina. E saper dire di "no" ai software troppo invadenti.

grand@hackerjournal.it

www.hackerjournal.it

HACKER JOURNAL

Saremo di nuovo in edicola Giovedì 13 Marzo!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

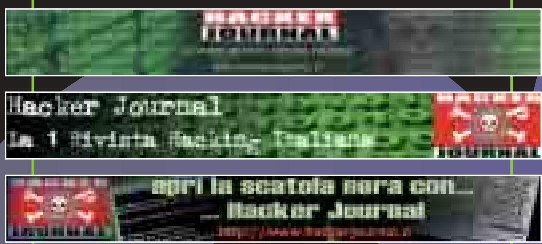
w w w . h a c k e r j o u r n a l . i t

DISEGNA I BANNER DI HJ!

Tanti siti Web ci hanno linkato e ci chiedono un banner. Abbiamo pensato di farlo creare a voi lettori. Il banner deve avere dimensioni 468x60 pixel.
Saranno tutti pubblicati sul sito (nella sezione Artwork, dal link sulla home page), e ognuno potrà scegliere il banner che preferisce!
Invia il tuo lavoro all'indirizzo:

banner@hackerjournal.it

I più belli e fantasiosi saranno pubblicati sulla rivista!
Qui potete vedere quelli scelti per questo numero.



DA LEGGERE SUL SITO

Tra gli articoli più interessanti, più letti o più commentati di questo periodo, sul sito di HJ trovate "Eliminare CyDoor", che spiega come rimuovere lo spyware installato da Kazaa e altri programmi, e la prima puntata di una nuova "Guida al Pascal" per principianti. Passando ad argomenti meno tecnici ma non meno interessanti, vi consigliamo "Aspetti Giuridici dell'Hacking" di Piranha.

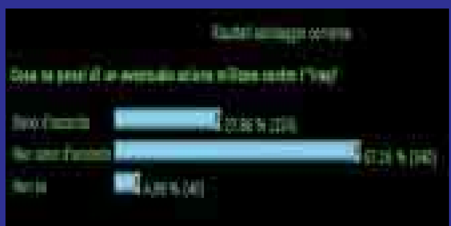
Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: bambo18
pass: cos3tto

SONDAGGIO

A differenza di quanto accadeva un po' di tempo fa, oltre a poter partecipare al sondaggio con la vostra risposta, potete anche esprimere commenti sul testo del sondaggio o sul suo risultato. Insomma, anche se non vi identificate con le risposte previste, o se volte fare precisazioni, avete comunque la possibilità di dire la vostra.



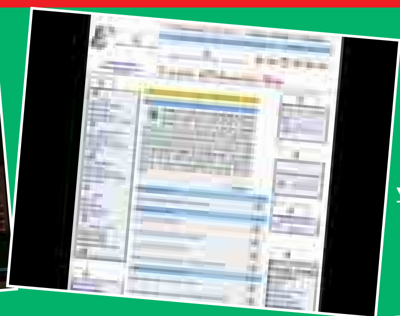
I 10 PROGRAMMI PIÙ SCARICATI

1. **Cleaner3.5** (Anti-Troyan, 3786 download)
2. **Genius** (Windows, 3006 download)
3. **EmailTracker** (Windows, 2504 download)
4. **Kerio2.1** (Firewall, 2478 download)
5. **SuperScan3.0** (Scanner, 2380 download)
6. **Uplink** (Windows, 2278 download)
7. **MultyProxy** (Windows, 1913 download)
8. **Camouflage** (Windows, 1853 download)
9. **Keyogger** (Windows, 1759 download)
10. **Intrusion Detection** (Intrusion Detection, 1623 download)

ECCO ALCUNI DEI VOSTRI SITI.
Se volete comparire in questo spazio, scrivete a: redazione@hackerjournal.it

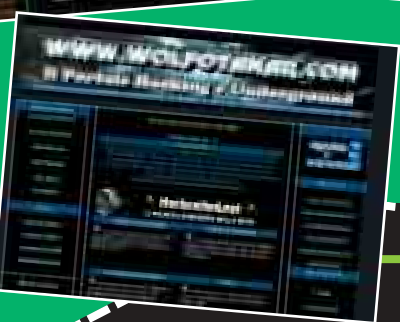
Dai bit alla carta

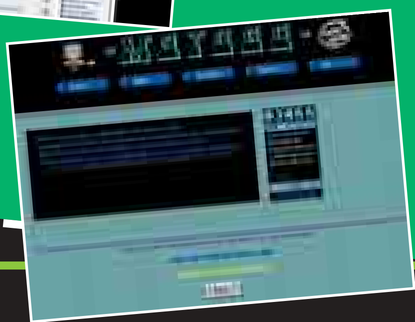




www.moto80.tk
www.wolfotakar.com
www.snipernorth.too.it
www.hackerspeed.too.it
www.playernet.org







HACKER JOURNAL

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

mailto:

redazione@hackerjournal.it

VIDEORIASSUNTO

Vorrei sapere se ci sono dei compressori .avi che da un file di circa 2GB riesce a portarlo a circa 700MB per fare un esempio quando si finisce la conversione di un file .vob con flask mpeg e dopo aver incollato l'audio con virtual dub bisogna farlo per forza in 2 cd io volevo farlo in 1 cd solo è possibile? Se è possibile mi fate un favorone da niente.

SCISM@85

Parto ovviamente dal presupposto che già sia stato utilizzato un codec DivX, che garantisce di ridurre drasticamente le dimensioni di un filmato mantenendo una buona qualità. Fatta questa precisazione, ti dirò che tutto è possibile, ma non senza dover scendere a qualche compromesso. Le dimensioni di un filmato possono essere ridotte in molti modi: variando la risoluzione, il frame rate (il numero di fotogrammi al secondo, che determina la fluidità del video), il rapporto di compressione, il codec utilizzato, il numero e la qualità delle tracce audio.
Molti programmi, anche gratuiti fanno queste conversioni (tra cui il FlaskMPEG che hai citato tu), ma nessuno potrà ridurre le dimensioni senza abbassare in qualche modo la qualità.

ALTRO CHE MEDIOMAN!

Aiuto!! Altro che Medioman, anche perché so omo e non mi aiuterebbe... Ho un mega probelma: sono on-line e Winzoz si resetta. Una volta, due volte, ogni venti minuti!! non so più che fare: antivirus e antitrojan aggiornati danno risultato nullo, ho contattato la Symantech ma non m'è stato d'aiuto; non posso accedere a msn.com per leggere la posta e passaport.net mi dice di abbassare il livello di protezione(?!?) ma resta inutile e non mi permette di usare messenger. Capita solo on line, mai off-line.

Metalized_blood

Viaggio a Lourdes? Reinstallazione di Windows? Meglio la seconda opzione...

PC CHE SI SVEGLIA DA SOLO

Il mio PC si accende da solo! Questo avviene solo se è collegato alla linea telefonica, e mi sta preoccupando non poco. Abbiamo sempre detto che l'unico PC al sicuro è quello spento, ok? Ma questo si accende da solo! Ho un Norton Corporate aggiornato, scansioni e LiveUpdate aggiornate, Trojan Remover scansioni ok, utilizzo zone Alarm come firewall, insomma sembra pulito. E allora? Il PC è un p4 2, 5 Hz. con XP Home, è entrato in casa da poco. Mi viene da pensare a un assemblaggio sbagliato; voi cosa ne pensate? comunque se non è collegato non ci sono problemi, se si attacca lo spinotto del telefono (a casa utilizzo una normale linea telefonica con modem interno generic softk56), dopo qualche ora sia di giorno che di notte mi ritrovo con il PC acceso, senza nessuna attività particolare o comunque evidente. Ho provato anche appena trovatolo acceso a verificare le connessioni, tramite il comando netstat e netstat -an ma non vedo nulla di strano.

OutSte

Molte schede madre supportano una funzionalità chiamata "Wake on modem", che permette di accendere il computer quando riceve una chiamata telefonica. Questo permette per esempio di collegarsi al computer da una postazione remota senza il bisogno di lasciarlo costantemente acceso. Probabilmente quando ricevi una telefonata, il computer risponde per te (o almeno ci prova), e ovviamente si "sveglia". Dovrebbe bastare entrare nelle impostazioni dei Bios (premendo Canc all'avvio del computer), e disabilitare questa funzionalità (ogni scheda madre è diversa, ma dovresti trovarla nella sezione Bios Features, o qualcosa di simile.

SUGGERIMENTI

Descrizione: salve sono un vostro assiduo lettore fin dal 1° numero di HJ e fin dal primo momento sono stato calamitato in edicola a comprarlo tutte le volte che esce ma la mia domanda o richiesta era: perché non mettere meno articoli ma spiegati nel migliore dei modi ? cioè : perché non mettere guide + dettagliate e complete su come difendersi da attacchi e soprattutto come contrattaccare !?!?!?!?!? questa richiesta credevo di trovarla col passare delle uscite quindi perché non insegnare un po' di tecnica pratica su intrusioni difesa ecc. a persone spesso vittime di quelli che credono essere Hacker ma che invece alla fine risultano essere sempre e solo L@mer ??? diamoci una mossa (Leggi permettendo !!!) AIUTIAMO QUESTE VITTIME ;)))

Atmospher

Purtroppo ci troviamo a dover cercare di fare una rivista il più possibile completa in sole 32 pagine, e non sempre è facile. Cercheremo comunque di far tesoro del tuo suggerimento.

☺ Tech Humor ☺



Super Computer Fan

Qualcuno ha esagerato con l'overclocking?

TROJAN REMOVER

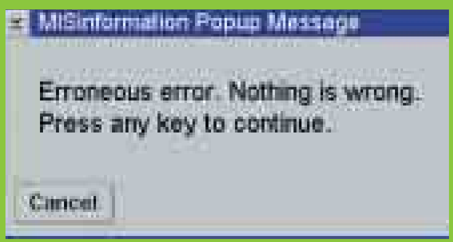
Gentile redazione,
ho scaricato da poco dal sito www.simplysup.com il programma Trojan Remover da voi "recensito" nel numero 17 di HJ. Nello stesso articolo avete però affermato che il mancato pagamento per la registrazione in linea non preclude il funzionamento del suddetto software, il che è vero ma... solo per 30 giorni! Penso che sarebbe giusto, al fine di scansare equivoci, ricordare ai lettori

che il programmino è disponibile in solo in *versione trial*!
Per il resto niente da aggiungere, continuate così : -)

Christi@n

Grazie per la segnalazione. Abbiamo provveduto a tirare le orecchie all'autore dell'articolo ;-)

☺ Tech Humor ☺



Errore erroneo. Non c'è niente che non va. Premi un tasto per continuare.

WORM

Credo di avere un worm come posso eliminarlo se è fondato il mio dubbio?

Adrians

Beh, con un Wormifugo :)
Scherzi a parte, un buon antivirus dovrebbe bastare.

POTENZA CONDIVISA

Nel vostro articolo sul peer to peer parlavate di sharing della potenza di calcolo dei computer collegati. In che maniera è possibile fare ciò? E lo si può fare con una rete peer to peer domestica?

Cattivik

Credo ci sia un'incomprensione di fondo. In quell'articolo si faceva riferimento a progetti come il Seti@home (http: //setiathome.ssl.berkeley.edu), che analizza i segnali provenienti dai radiotelescopi alla ricerca di eventuali comunicazioni aliene, o Distributed.net (www.distributed.net), che cerca di violare i più complessi algoritmi di cifratura. In questi casi, le cose funzionano così: l'enorme mole dei dati da trattare viene suddivisa in tanti segmenti; ogni segmento viene inviato alle migliaia di client installati su computer di laboratori, scuole o utenti comuni; il PC elabora i dati, restituisce il risultato, e poi scarica il successivo segmento. Dalla tua domanda, mi pare di capire che tu voglia utilizzare più computer per effettuare una tua elaborazione. Anche questo si può fare, ma non è semplicissimo. In questo modo, per dirne una, alcuni studi cinematografici fanno le elaborazioni digitali dei film.
Su http: //parallel.rz.uni-mannheim.de/Linux/parallel/Sites/Index.html trovi una serie di link a università o altre istituzioni che hanno creato sistemi di elaborazione parallela.

☺ Tech Humor ☺



Se a colazione siete già ridotti a questo stadio, vuol dire che siete messi davvero male.

ARGOMENTI CONCRETI

Ciao, per prima cosa mi voglio complimentare con voi perché avete messo su due riviste formidabili e poi volevo darvi qualche suggerimento. Voi già avete riscosso un grande successo e veduto molte copie ma secondo me potreste venderne di più mettendo nella rivista articoli più concreti e in modo comprensibile non solo ai professionisti ma anche agli apprendisti che hanno appena iniziato. Ad esempio potreste fare un articolo su come usare netbus, come infettare la vittima con netbus, come camuffare il trojan di netbus... Insomma un articolo che dopo averlo letto io so perfettamente entrare nel PC di una persona da me infettato e fatto tutto da me. Avete capito cosa voglio dire? Ciao e grazie per l'ascolto.

Snogontek

Sì. Ho capito benissimo. Parli di tutti quei comportamenti che gettano fango sulla categoria degli hacker, e che fanno crescere l'incazzatura della gente... Di tutte quelle cose che tu non vorresti mai che un altro facesse a te.

Errata corrige

Per un errore di stampa, sono saltate alcune righe dall'articolo "Come ti nascondo il file", all'inizio di pagina 14 del numero scorso. Ecco il pezzo scomparso:

Scomponendo in bit i byte dell'immagine abbiamo come valore dell'ultimo bit di ciascuno di essi i
seguenti valori [1] [1] [1] [1] [1] [1] [0] [0].
Il programma da realizzare dovrà quindi variare l'ultimo bit dei byte dell'immagine al fine di inserire i bit che, una volta messi insieme a otto a otto, daranno i byte corrispondenti al carattere del testo da nascondere.
I byte dell'immagine finale potranno quindi avere dei valori diversi da quelli originali e più esattamente: [144] [211] [84] [98] [77] [177] [249] [219].
Alla fine del processo si ha la stessa immagine in cui se il valore del byte in esame è un numero pari, esso rappresenta - nella fase di ricostruzione del testo - un bit con valore "0", alrimenti "1".
Sulla base di queste descrizioni, ecco di seguito cosa deve fare il programma per inderire o estrarre il testo da una immagine. Volutamente si è scelto di non indicare il listato di un linguaggio specifico bensì di indicare le istruzioni in modo comprensibile a tutti così che chi vorrà realizzerà il suo programma nel linguaggio che meglio conosce.

NEWS

HOT!

IL BUCATORE BUCATO

Kevin Mitnick, quello che si può proverbialmente definire l'hacker più famoso del mondo, ha messo la testa a posto: non appena riguadagnata la libertà, si è dedicato a un lavoro "pulito", fondando la società di consulenza Defensive Thinking. Ma il sito societario, www.defensivethinking.com, è stato rapidamente violato da un cracker noto come BugBear. Il server non ha riportato particolari danni, ma ben più grave è stato il danno d'immagine. BugBear ha firmato la sua impresa con un beffardo messaggio, che recitava più o meno "Bentornato! Per darti il benvenuto, abbiamo violato il tuo sito. PS In galera ci siamo dimenticati un po' di cosine sulla sicurezza, vero?"
La reazione di Mitnick è stata apparentemente molto blanda. Ha commentato che secondo lui si tratta solo di un omaggio di dubbio gusto, nulla più che un avvertimento, ma ha anche candidamente ammesso che il suo sistema mancava di svariate patch di sicurezza fondamentali che, si è affrettato ad aggiungere, sono state immediatamente approntate.

DYNEBOLIC, LINUX SU UN CD

E'stata rilasciata la prima versione "stabile" della distribuzione Linux DyneBolic (http://dynebolic.org/). La caratteristica principale e più interessante è il suo essere eseguibile tutta da un CD, senza bisogno di hard disk. In generale, la distribuzione è piuttosto incentrata sulla multimedialità, sia passiva che attiva: sono infatti comprese utility per lo streaming audio e video. L'immagine del Cd è, nemmeno a dirlo, liberamente scaricabile dal sito ufficiale.



IPOD CON UN CUORE DI LINUX?

Fra gli audaci esperimenti di porting condotti dalla creativissima comunità di sviluppatori Linux ne troviamo uno che potrebbe sembrare estremo anche agli occhi del guru più incallito: la linuxizzazione del glamouroso iPod, ovvero: come ti faccio girare un Linux piccolo piccolo anche nel player Mp3 più alla moda in questo momento. L'autore del miracolo si chiama Bernard Leach, ed è opera sua il porting su iPod di uClinux, una versione embedded di Linux.
Seppure il progetto sia ancora embrionale, la versione di Linux per iPod dispone di funzionalità di base per la gestione del frame buffer, del dispositivo audio, dell'interfaccia di input ed un supporto rudinmentale all'hard disk e al file system FAT, quanto basta per controllare le funzionalità di base del player. Sono attualmente allo studio, fra gli altri, il supporto alla rotellina e alla porta FireWire.
Una volta completato, il progetto potrebbe davvero costituire una seria alternativa al firmware di Apple, ma l'autore non nega che si tratta di un lavoro lungo e difficile, reso ancora più complesso dalla mancanza di documentazione tecnica, in base al principio secondo cui Apple considera iPod una piattaforma totalmente chiusa.



POLIZIA TAILANDESE BEFFATA DAI DEFACER

Il sito http://legal.police.go.th, come più di un centinaio di altri siti ad esso connessi e ugualmente legati alle forze dell'ordine tailandesi, è stato colpito da un defacement da parte di un cracker noto come afka, membro del gruppo francese "T.I.G.", che finora aveva firmato solo sporadici attacchi di portata limitata. In questo caso si tratta invece di uno dei defacement più massicci mai portati a termine nella storia del cracking.

SEMAFORI CON IL TELECOMANDO

Nel Regno Unito si è diffusa a macchia d'olio la notizia, riportata anche da alcuni quotidiani più o meno autorevoli, secondo la quale un sito Web riporterebbe informazioni piuttosto dettagliate su come "telecomandare", letteralmente, il sistema semaforico londinese. Secondo le indiscrezioni, basterebbe una connessione wireless e un laptop per far scattare il semaforo nel modo più favorevole, ma non solo. Si parla anche di aggirare controlli di pubblica sicurezza o "dirottare" interi gruppi di semafori, si forniscono specifiche tecniche e glossari per addetti ai lavori, fino ad arrivare a veri e propri cracking della rete di controllo. Gli strumenti necessari a fare tutto questo, oltre a quelli già citati, sono di reperibilità difficile ma non impossibile; e questi dati, la cui incauta manipolazione potrebbe facilmente creare il caos, se non anche incidenti piuttosto gravi, secondo gli esperti provengono necessariamente dall'interno della rete di addetti alla gestione del traffico londinese.

NUOVA RELEASE DI DIVX

E'stata appena rilasciata la versione 5.0.3 del codec di estrazione video DiVX, ottimizzato per Pentium 4 fin dalla versione 5, che migliora le prestazioni complessive e corregge alcuni bug presenti nelle precedenti release. La nuova versione del codec, in bundle con il relativo player, è scaricabile, in tre differenti pacchetti (gratuito, adware e shareware) presso il sito ufficiale, www.divx.com.



VENT'ANNI PER UN KEYLOG

Sembra una storia come tante altre: uno studente un po' più smanettone degli altri installa un keylogger sulle macchine dell'aula informatica, per andarsi a sbirciare cosa mai scrivono i suoi compagni quando sono nascosti dietro a un monitor (ma non solo, a essere sinceri: si parla di utilizzo fraudolento di numeri di carta di credito e "visitine" agli account altrui mediante furto di password). Un po' meno banale è il provvedimento che è stato preso nei suoi confronti; l'accusa di aver violato ben sette normative federali, fra cui intercettazione illegale di comunicazioni elettroniche e accesso non autorizzato a sistemi informatici protetti. Ma il reato più grave è quello che sembra il più banale: siccome l'installazione fraudolenta è avvenuta di notte, entrando di soppiatto nei locali dell'università, si parla solo per questo di una pena che può raggiungere i vent'anni di prigione.
La condanna rappresenterebbe una punizione smisurata e un precedente inquietante, e a tal scopo l'università stessa sta cercando di mediare, assicurando che lo studente ha utilizzato a titolo esclusivamente personale i dati trafugati, senza rivenderli o condividerli con altri.

SEMBRA CNN MA NON È



Una bufala inventata da uno studente statunitense ha fatto passare momenti un po' cupi nientemeno che a Cnn, Vivendi e Microsoft. Come ci è riuscito? Realizzando sul proprio spazio web universitario una pagina Web del tutto simile a quelle del sito Cnn, che riportava la (falsa) notizia dell'acquisto di Vivendi International da parte di Microsoft. La pagina è stata rimossa velocemente, ma pare abbia suscitato imbarazzo tale da mettere in guai seri l'incauto studente, nei confronti del quale sia Cnn che Microsoft potrebbero rivalersi per un risarcimento danni. Del resto la notizia non è così assurda: l'interesse della casa di Redmond per l'azienda videoludica francese non è un segreto.

XBOX PRECIPITA, OFFICE DECOLLA



Xbox non si può proprio dire essere stata un grande successo: le perdite ad essa relative sono ulteriormente raddoppiate nell'ultimo trimestre del 2002. Più precisamente, si parla di una perdita di 248 milioni di dollari, quantificabile, al lato pratico, in una perdita di 100 dollari per ogni console da 199 dollari venduta. D'altro canto, Office si è rivelato essere la vera colonna portante dell'azienda, e chiude in attivo assieme al settore piattaforme server, in un quadro complessivo di leggero calo di fatturato.

PC IN REMOTO SUL CELLULARE



Il nuovo modello di cellulare P800 di Sony Ericsson supporterà il software Remote Control, già disponibile sul mercato, e consistente in una suite di applicazioni per il controllo remoto del Pc. Mediante Remote Control si potrà collegarsi al pc locale, modificare un documento e compiere operazioni intervenendo sull'interfaccia (per riavviare il computer, ad esempio).
Ma si potrà anche intervenire sul server, per leggere e inviare email e fax e controllarne il corretto funzionamento.

HOT!

DAGLI ALL'UNTORE! O FORSE NO...

La notizia era delle più succose: il ritrovamento dell'autore del famigerato Slammer, il virus che ha messo in ginocchio le Poste Italiane. Si sarebbe trattato di un fantomatico Abu Mujahid, membro del gruppo pakistano Harkat-ul-Mujahadeen, che avrebbe causato il ben noto disastro inment di una presunta cyberjihad a sostegno di al-Qaeda. La notizia era stata suffragata e diffusa da testate autorevoli, fra cui Computerworld, che ne aveva fatto un titolo di testa della sua newsletter. Ma dopo poche ore la notizia è stata rimossa dal sito (la newsletter, ahimè, era già partita) e al suo posto è apparsa una nota, che accennava a "dubbi sull'autenticità della notizia". Di lì a poco si è appresa tutta la verità: Abu Mujahid altro non era che Brian McWilliams, un giornalista freelance che collabora, fra le altre, con le prestigiose Salon e Wired, che ha voluto dare all'intraprendente intervistatore una lezione perché lui (e altri colleghi altrettanto incauti) imparassero a usare un po' meno entusiasmo e un po' più di raziocinio a trattare i casi di cyberterrorismo. Sul sito www.harkatulmujahideen.org, utilizzato per la beffa, ci sono ora tutti i dettagli dell'operazione.

IL CELLULARE CHE TI CASTIGA

Ok, speriamo che resti solo una trovata pubblicitaria, e che a nessuno venga mai in mente di produrli. Stiamo parlando di alcuni concetti di design industriale proposti dalla Ideo (www.ideo.com), che ha progettato dei cellulari che consentono di infliggere punizioni a chi fa uso improprio del telefonino. Stiamo parlando di avvisi perentori, ma anche e soprattutto di punizioni fisiche, nella fattispecie scosse elettriche, che potrebbero variare di intensità al reiterarsi o al peggiorare del comportamento molesto. Secondo gli ideatori del discutibile dispositivo, la rabbia della gente per i maleducati del portatile è tanta e tale che solo una punizione fisica potrebbe realmente dare soddisfazione. Dichiarazione forse condividibile da alcuni, ma pericolosissima da mettere in pratica. Nessuno invece ha ancora inventato una tastiera che morda chi inoltra le catene via email. Purtroppo.

HOT!

CRACKER ALL'UNIVERSITÀ DI MILANO

E' stata resa nota una importante violazione ai danni dell'Università di Milano, più precisamente a un gruppo di sei siti, attaccati dal gruppo di cracker brasiliani d0ne, e sottoposti a defacement con l'inserimento di una immagine e un messaggio di rivendicazione. I siti, tutti appartenenti al subdomain dico.unimi.it, sono attualmente stati ripristinati, ma ancora non visibili.



SUPERPATCH PER XP E IE

Sono state recentemente individuate tre falle piuttosto gravi a carico dei prodotti di casa Microsoft. Le prime due riguardano Internet Explorer, e più precisamente il modello di sicurezza cross domain, quello che dovrebbe impedire alle aree di due differenti domini di condividere informazioni. Ma apparentemente uno dei controlli di sicurezza di IE contiene le succitate falle, che permettono quindi a un sito Web di accedere alle informazioni di un altro dominio quando si utilizzato determinate caselle di dialogo.
Va da sé che è sufficiente creare un sito Web ad hoc per poter sfruttare queste falle, eseguendo script maliziosi sul computer dell'utente per accedere ad altri domini, nonché lanciare file eseguibili presenti in locale.
Windows Update è già aggiornato, e correggerà automaticamente questa falla. La patch ufficiale, scaricabile come di consueto mediante il link presente nel bollettino, è cumulativa, e contiene tutti i fix di sicurezza rilasciati fino a quel momento per le 5.x e 6.
A questa falla, classificata come "critical", ne segue una di livello "important", che riguarda Windows Redirector per Windows XP, ovvero una applicazione utilizzata per accedere a file locali e remoti indipendentemente dal protocollo di rete in uso. La falla consiste in un buffer non verificato e può essere sfruttata per eseguire del codice sul sistema locale (ma secondo Microsoft tale opportunità non può comunque essere sfruttata in remoto).

IL 12 MARZO DEBUTTA CENTRINO

La nuova linea di processori di Intel, dal nome per noi italiani così vezzoso (ma già nota come Banias) è destinata ad aprire una nuova era nel campo dei computer laptop. Si tratta di Cpu a frequenze di clock inferiori di quelle dei recenti P4-M, ma che lavorano a basso consumo (con notevole risparmio delle batterie) e dispongono di Wi-Fi integrato, concepiti quindi per il mobile computing wireless. Per la verità, quindi, è più proprio parlare di piattaforma, piuttosto che di singolo processore, trattandosi di un vero e proprio sistema integrato. Anche il controllo del risparmio energetico non si limita alla Cpu: alcune parti del Bus possono funzionare a voltaggio limitato, e le istruzioni in arrivo vengono gestite dal Dedicated Stack Manager, che le gestisce via hardware in modo che non interrompano il lavoro in corso da parte del processore.
Notevoli anche le sue prestazioni nel campo multimediale, soprattutto nella compressione video.
Le prime frequenze disponibili saranno 1,3, 1,4, 1,5 e 1,6 GHz, con 1 Mbyte di cache integrata.

CHI ORIGLIA NEL P2P

Big Champagne, una società statunitense specializzata in ricerche di mercato e consulenze di marketing, ha trovato un canale nuovo per il suo lavoro: il peer to peer. In parole povere, attraverso un software realizzato ad hoc va a sbirciare il traffico dei vari network di file sharing e analizza quali sono i file più ricercati e più scambiati, più introvabili nelle varie parti del mondo.
I numeri (e i nomi) coinvolti in questo peculiare data mining sono notevoli: si parla di 25 milioni di ricerche al giorno su 20 milioni di utenti di eDonkey, DirectConnect, FastTrack, iMesh, Overnet, Ares, Blubster, Gnutella, Overnet, Ares, Filetopia e FileNavigator.
I responsabili dell'azienda, interpellati in merito, trovano tutto ciò molto normale. Peccato che siamo davanti a un qualcosa che supera i limiti del tradizionale spywaring, e che sfrutta scambi illegali (ovvio che a Big Champagne non interessa quante foto delle vacanze di ci scambia via Gnutella) andando letteralmente a frugare nei dischi fissi degli utenti.

BearShare® The Power To Share

AMORE FRA VODAFONE E HOTMAIL

In Gran Bretagna l'offerta di servizi di rete di Vodafone è stata recentemente integrata da una partership con Microsoft, che attraverso i servizi Hotmail, consentirà di verificare la mailbox alla ricerca di nuovi messaggi di posta, nonché di controllare la presenza online di contatti Messenger, tutto mediante il telefono cellulare. Non è per il momento ancora noto se Vodafone intende esportanre anche in Italia tale servizio.

NON SEI A SCUOLA? SQUILLINO AI TUOI

I preside di tre licei in provincia di Pisa ha ideato un modo quantomeno originale per avvisare i genitori delle assenze dei figli da scuola: il famigerato squillino. Se mamma o papà troveranno il numero della scuola sul loro display, capiranno che c'è qualcosa che non va. Questa iniziativa si aggiunge ad un'altra, precedente e altrettanto rivoluzionaria: la creazioen di un sito Internet nel quale, mediante accesso con password a un'area riservata, i genitori possono consultare il registro di classe.

MOTOROLA E LINUX INSIEME SUGLI SMARTPHONE

E' in arrivo da Motorola quello che si preannuncia come un prodotto interessante non solo dal punto di vista meramente consumistico (uno smartphone di ultima generazione), ma anche per l'innovazione tecnologica che porta con sé: la combinazione di Linux e tecnologia Java. Linux è già stato visto in versione embedded su device mobili, fra cui il più noto è senz'altro il modello Zaurus di Sharp. Ma l'applicazione di Linux nel campo della telefonia mobile è una novità assoluta, se si esclude una vaga espressione di intenti formulata tempo fa da Nec.
Il nuovo smartphone, denominato A760, dotato di schermo a colori, combinerà tutte le funzionalità di un telefono mobile e di un Pda, e implementerà il supporto video e audio digitale in acquisizione e riproduzione, la messaggistica istantanea, la navigazione Web e sarà dotato di supporto Bluetooth.
L'A760 è previsto in arrivo sul mercato asiatico per il terzo trimestre, e successivamente negli Stati Uniti e in Europa.

CASA CONNESSA AL CEBIT 2003

Philips rilancia le sue offerte per la "casa digitale", preparando molte novità per il CeBIT, la più importante manifestazione a livello mondiale, che si svolgerà ad Hannover dal 12 al 19 marzo.
Il suo modello di casa digitale comprende una irrinunciabile connessione a banda larga e una serie di dispositivi connessi ad essa e fra di loro tramite cavi o connessione wireless. L'accento sarà posto in particolar modo sui dispositivi portatili, fra cui iPronto, una sorta di telecomando che potrà governare a distanza tutti i dispositivi della casa mediante connessione WiFi, con le funzioni di un vero e proprio Pda, compresa la possibilità di connettersi a Internet.
Un'altra novità per il CeBIT è un ricevitore wireless digitale multimediale con tecnologia WiFi, il primo nel suo genere, per la connessione fra computer e home theatre, in modo da poter utilizzare i contenuti multimediali per Pc sul sistema casalingo.
E poi ancora DesXcape, un monitor a colori a cristalli liquidi da 15 pollici anch'esso a colori, attraverso il quale si può accedere ai contenuti del proprio Pc mediante connessione wireless.

INTEL SI SCATENA SUL PORTATILE

Nonostante gli sforzi profusi nel progetto Centrino, Intel non resta con le mani in mano nel settore wireless, rilasciando un processore espressamente dedicato ai telefoni cellulari, basato sulla tecnologia proprietaria Wireless-Internet-on-a-chip. Nome in codice Manitoba, noto anche come PXA800F, integra su un'unica piastrina tutti i principali componenti del dispositivo, ovvero comunicazione, elaborazione dati e memoria, mediante la tecnologia a 0,13 micron, consentendone così un design più ergonomico e una maggiore durata della carica.
PXA800F è un processore a 312 MHz in tecnologia XScale con 4 Mbyte di memoria flash e 512 Kbyte (KB) di SRAM. Comprende un processore di segnale a 104 MHz basato sull'architettura MicroSignal con 512 KByte di memoria flash Intel On-Chip integrata e 64 KByte di SRAM. Dovrebbe essere implementato sui dispositivi portatili a partire dalla fine del 2003.

HOT!

STAMPANTE PER CD DA EPSON

L'ultimo nato in casa Epson è espressamente pensato per gli utenti home che si dilettano di fotografia digitale e elaborazioni multimediali in genere. Stylus Photo 900, stampante inkjet a sei colori, stampa fino al formato A4 in qualità fotografica, con supporto alla carta in rotolo per una resa del tutto simile a quello delle foto tradizionali. Il software in dotazione consente inoltre di realizzare copertine per i Cd e i Dvd, combinando testo, immagini e eventualmente loghi di società. Il prezzo è di 208 euro, Iva esclusa.

CELLULARI ESPLOSIVI

La notizia è frivola (beninteso, con il dovuto rispetto verso chi è rimasto ferito), ma ha sollevato molto polverone: un cellulare è letteralmente esploso fra le mani del suo utilizzatore, ferendolo al viso con le schegge del display. Si sta indagando sugli apparecchi dello stesso lotto di quello incriminato, per verificare eventuali difetti di produzione. Il problema pare risiedere in un malfunzionamento della batteria, acquistata e sostituita di recente, associata ad una lunga esposizione del dispositivo a una fonte di calore.

LA SOTTILE VENDETTA DI OPERA

Qualche settimana va gli autori di Opera hanno scoperto che il link che dal portale Msn avrebbe dovuto portare al proprio sito aziendale finiva nel nulla: ultimo evento fra tanti boicottaggi più o meno volontari. Come burlesca ritorsione verso Msn, Opera ha rilasciato una versione molto speciale del suo browser, la Bork edition, che prende il nome dal cuoco svedese che è uno dei protagonisti del Muppet Show.
Non c'è alcuna differenza rispetto alla versione tradizionale, tranne che per un sito: Msn. Puntando a tale url, tutta la pagina verrà visualizzata nel linguaggio del suddetto personaggio, ovvero un susseguirsi di Bork, Bork, Bork.

INTERVISTA A MARCUS J RANUM, UNO DEI PADRI DEL FIREWALL

L'uomo dei firewall

Lo abbiamo incontrato Durante la manifestazione Infosecurity di Milano, e gli abbiamo fatto qualche "innocente domanda".

Marcus J Ranum è uno dei più famosi progettisti informatici per la sicurezza e l'autore principale di numerosi firewall, tra cui il Dec Seal, il TIS Gauuntlet e il TIS Internet Firewall Toolkit. Ha lavorato per più di tredici anni presso la Unix Networking and Security Community come ingegnere informatico, manager di sistema e consulente, maturando una grande esperienza come progettista e sviluppatore di sistemi per la sicurezza delle reti. Come se non bastasse di recente ha contribuito alla progettazione di whitehouse.gov



Ranum è anche appassionato di fotografia, potete trovare diverse opere nel suo sito: www.ranum.com

HJ - che cosa ne pensi degli hacker?

Bisogna distinguere tra hacker e hacker. C'e una varietà di terminologie, tra hacker, cracker, lamer… A me piace usare definizioni ancora diverse, perché anche il termine hacker è stato rovinato dalla stampa. A me piace dire: "È cosa da geek".
Oppure: "È cosa da tecnofilo". Sono totalmente a favore di coloro che amano mettere le mani nei computer, vedere come funzionano, gente alla quale piace costruire cose interessanti, alla quale piace capire la tecnologia. Il punto in cui io traccio la linea è quando qualcuno crea strumenti che intenzionalmente distruggono. Io credo che ci sia una questione morale; se io metto una serratura è perché non voglio che entri qualcuno. Il fatto che la serratura sia difettosa non cambia. Qualcuno entra lo stesso e dice: "Guarda che la tua serratura era difettosa, sono entrato". Io credo che sia sbagliato. Le serrature esistono per permettere alle persone oneste di rimanere tali.

HJ - Hai mai copiato un programma?

Si, ho usato software pirata. Puoi citare questo fatto. Quando ho cominciato a interessarmi di fotografia, ho piratato una copia di Photoshop perché volevo vedere se andava bene. Ovviamente avrei potuto usare una versione "light" o di prova, ma volevo vedere come funzionava la versione completa. Un anno dopo l'ho comprato perché lo usavo molto. Se ho installato un software pirata e l'utilizzo poco, lo cancello e non pago. Se l'utilizzo, diciamo, almeno una volta al mese, lo compro.

HJ - Siamo d'accordo che un hacker che tira giù grandi sistemi e fa danni è da condannare, ma uno che entra in un sito, spiega al webmaster quali sono le falle dalle quali ha ottenuto accesso…

E' sbagliato! Io credo sia sbagliato. Questo è il problema che ho con gente come Adrian Lemo… Nessuno lo ha invitato. Se io vengo da te e ti dico: "Prova a entrare nel mio sito", e tu ci provi, è una questione. Se tu semplicemente ci

provi senza invito è diverso. È come se io andassi a casa tua senza il tuo permesso. Non è giusto, è imbarazzante, e danneggia. Può costare il lavoro a qualcuno. È il rovescio della medaglia di tutta questa storia degli hacker; per ogni Adrian Lemo che diventa famoso perché si è intrufolato nel sito del New York Time, c'è un amministratore di sistemi che ha una vita, bambini che vanno a scuola, rate da pagare per la macchina e per l'appartamento. Ora è disoccupato perché uno stronzo si è introdotto senza permesso. Non e' giusto!

HJ - Molte case software approfittano che ci siano persone che testano i programmi o siti per loro; non hanno il budget per fare testing, vendono prodotti non finiti che qualcuno, hacker o no, testerà...

Per prima cosa diciamo che una società che vende software senza testarlo sbaglia. Se ti vendo qualcosa che non credo sia di buona qualità, io sono uno stronzo. Ci sono molte società che lo fanno. È giusto incolpare le case di software che vendono merda. Io do la colpa a tutti. Do la colpa agli utenti stupidi che comprano quel software, alle case di software stupide, e agli hacker stupidi che trovano i problemi e li rendono pubblici in una maniera che danneggia gli utenti. L'ideologia e le ragioni per le quali un hacker ha avuto la possibilità di mettersi nella posizione di farti un piacere è dovuta ad alcune società, come Microsoft, che dicevano: "non e' un bug". È come se io ti vendessi una macchina sapendo che il volante non funzionerà ad alta velocità, ma dico che non c'e' nessun problema. È moralmente sbagliato. Molti hacker mi vedono come anti-hacker, e a favore dei produttori di software. Io sono molto anti-hacker (nel senso di cracker), ma sono altrettanto contro il cattivo software.I venditori dovrebbero essere punibili per cattivo software e gli hackers dovrebbero essere punibili per l'hacking. Gli unici innocenti sono i poveri clienti.



HJ - Credi davvero che ci siano organizzazioni che fanno incursioni mirate con scopi politici o militari?

Sì! Un amico, al quale credo, dice che i Cinesi hanno grandi capacità offensive nel campo informatico. Al Pentagono alcuni volevano sviluppare tecniche d'offesa informatica. Il presidente Bush ha dato l'OK. Credo che la guerra informatica sia un'idea stupida. Vuoi distruggere qualcuno? Chi può fare più danni dell'Enron? Non si capisce perché distruggere il mio sistema bancario quando potresti distruggere la mia economia diventando il presidente di una grande società. Per danneggiare gli USA, Bin Laden avrebbe dovuto fare come la Enron, invece di uccidere 3000 persone. Non credo che la guerra cibernetica sia un'arma d'attacco valida, forse tra dieci anni. Non è ancora il momento. I sistemi sono ancora troppo incompatibili... Non credo che i reattori nucleari siano ancora connessi a Internet... I missili balistici non sono connessi a Internet... È tutta tecnologia degli anni '60, non capisce il protocollo TCP/IP. Forse in dieci anni, la prossima generazione di tecnologia militare... Allora sì che avrò paura.

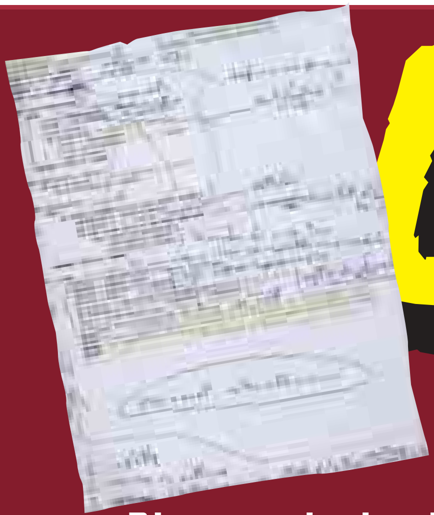
HJ - I firewall sono molto diffusi; sono sufficienti?

Fintanto che gli utenti possono installare software, i firewall sono limitati in quello che possono fare. Basta inviare un programma dicendo che apparirà Anna Kournikova nuda che tutti lo faranno girare. E quel programma non verrà fermato dai firewall. Inoltre, se tutti usano lo stesso firewall e qualcuno trova una contromisura che funziona con quello specifico firewall, siamo tutti vulnerabili. La stessa cosa vale per i software antivirus, se tutti usano lo stesso software antivirus il primo worm che aggira quel software può azzerare tutti i computer del mondo. Abbiamo bisogno di 60 diversi software antivirus e ognuno deve usarne uno diverso, non importa quale. Se qualcuno scrive un programma che sorpassa con successo 2, 3 o 4 antivirus, quelli che stanno usando un antivirus strano, che nessuno ha mai visto prima, sopravvivono. Una volta io mi occupavo di www.whitehouse.gov (il sito del Presidente USA, ndr). Usavamo un mailer che nessuno aveva mai visto prima e che nessuno ha mai visto da allora. Non aveva nessuna delle vulnerabilità degli altri mailer. Aveva i suoi difetti (e infatti ne ho scoperto uno un paio di anni dopo). In quel caso io ero immune a malattie che altri potevano prendere. A ogni nuovo baco trovato in sendmail (il più diffuso server di posta su Unix, ndr) io ero tranquillo. Stiamo raggiungendo un momento in cui la sicurezza dei computer è quasi biologica. Se vuoi costruire un Web server sicuro, la cosa migliore da fare è di prendere un qualche strano hardware, farci girare un qualche sistema operativo strampalato, e scrivere il tuo Web server. Non usare Apache, non usare IIS, scrivi il tuo. Non rendere pubblici i file sorgente. Perché trovare un problema di buffer overflow attraverso un network per un software di cui non hai i file sorgente è un lavoraccio. Ma trovarlo nel codice sorgente di Apache è molto più semplice. Quindi, dire che ognuno dovrebbe avere un firewall è un passo, ma in realtà ognuno dovrebbe avere firewall diversi.

HJ - Cosa intendi per "aspetto biologico"?

Da bambini tutti noi abbiamo ricevuto vaccinazioni per la rosolia, il vaiolo, il morbillo. Intorno al 1972 hanno smesso di vaccinare per il vaiolo perché pensavano che fosse stato sradicato. Poi abbiamo scoperto che l'Iraq l'aveva, che i russi l'avevano... E probabilmente anche Israele l'aveva. Il vaiolo potrebbe tornare; ogni persona con meno di 30 anni, che non è stata vaccinata, potrebbe morire. La stessa cosa si può fare con computer. Tutti usano lo stesso sistema operativo; tutti muoiono insieme. Quello che si può fare col software antivirus è molto interessante. Diciamo che ognuno di noi lavora per una diversa casa produttrice di software antivirus. Chi, tra noi si ammala per primo ha la chiave per riconoscere quel virus, per creare un vaccino. In pratica noi potremmo distribuire vaccini digitali in tempo reale. È qualcosa che non possiamo fare in natura. Questa è la direzione verso la quale ci dobbiamo muovere nel campo della sicurezza.

I VIRUS COME FORMA DI ESPRESSIONE ARTISTICA



UN'ARTE



Divorando testi epidemiC sui virus come strumenti di creazione artistica e di comunicazione, sul viruscode come atto poetico e allo stesso tempo rivoluzionario, un dubbio contagia, una visione infetta: forse Dio per creare il mondo ha scritto un codice sorgente?

Catch me if you can. Il messaggio trasmesso dal primo virus in assoluto, apparso sui monitor degli utenti collegati alla rete ARPAnet nel 1970, indicava l'identità del "germe", Sono Creeper, e una sfida, **"prendimi se ci riesci"**. Con il tempo l'identità dei germi è cambiata, ma la sfida è la stessa. L'ultima risale a lunedì 27 gennaio, quando **il worm SQL Slammer ha colpito (qualcuno ha precisato "ha punito") le Poste Italiane**, bloccando 14mila sportelli e creando disagi non solo agli utenti, ma anche ai dipendenti. Immediata la reazione dei media: il "male" ha colpito ancora! Pochi giorni dopo, invece, un altro virus **ha dato il nome a un evento ed è diventato, parte integrante di un museo** e segno indelebile della memoria culturale dei nostri tempi. All'-Haus der Kulturen der Welt (La Casa delle Culture del Mondo) di Berlino, in occasione della transmediale 0.3, uno dei più importanti festival del multimediale, si è tenuta infatti **"I love you – computer_viruses_hacker_culture"**, un'esposizione di Digitalcraft sui virus informatici.



BIENNALE DI VENEZIA

[2001 – Biennale d'Arte di Venezia]
In occasione dell'invito alla 49esima Biennale d'Arte di Venezia, i0100101110101101.ORG e gli epidemiC ideano e compilano il virus biennale.p. Il codice sorgente stato reso pubblico e diffuso il giorno dell'apertura della Biennale, 6 giugno 2001, dal Padiglione della Repubblica di Slovenia.

VIRII VIRUS VIREN VIRY

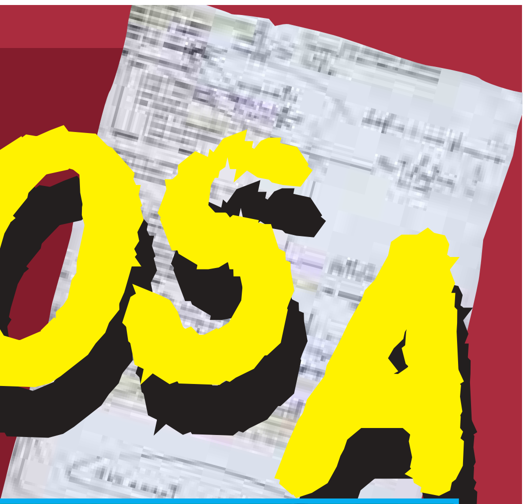
digital_is_not_analog.01
[2001 – Salara, Bologna]
Prima mostra sui virus mai realizzata fuori e dentro la rete, organizzata dagli epidemiC nel maggio 2001 in occasione di digital_is_not_analog.01 a Bologna (Salara).
www.d-i-n-a.org

>> L'arte del virus

I virus fanno parte del nostro patrimonio collettivo già da tempo, ed è forse proprio per questo che hanno suscitato l'attenzione di un museo. Partecipano attivamente alla nostra vita (al computer) dal 1986 da quando cioè Basit e Amjad svilupparono **Brain, il primo virus in ambiente Dos** e Ralf Burger presentò alla conferenza del "Chaos Computer Club" il suo **Virdem, un virus dimostrativo che infettava tutti i file com**. È solo di recente, però, che siamo davvero coscienti dell'esistenza di questi esseri digitali e del loro potere di auto-replicarsi, e cioè da quando, quel 3 maggio 2000, un messaggio di posta elettronica con oggetto I Love You (di qui il nome appunto dato all'esposizione di Berlino), con allegato il file "LOVE-LETTER-FOR-YOU.TXT.vbs", **colpì 300.000 sistemi in meno di 24 ore, mise KO i**

CONTAGIOSA





computer di banche, grosse società e persino di alcuni parlamenti. Alcuni virus si erano già diffusi sulla rete prima di quella data – basti pensare a Melissa -, ma **per la prima volta i media parlavano di danni notevoli**. Da quel giorno i virus animano le nostre paure digitali. A renderle più intense, a radicare in noi l'idea che siano solo delle brutte infezioni e rappresentino una minaccia economica, a mantenere alta la tensione mediatica sul fenomeno, **le case antivirus che rilasciano periodicamente terrificanti bollettini di guerra** oltre che gli "anticorpi" per bloccare e distruggere l'azione dell'antigene digitale, il corpo estraneo.



Digitalcraft ha avuto il merito di proporci invece una diversa visione del fenomeno, ponendo l'attenzione sull'intera natura del virus e non solo sui suoi aspetti negativi. Dopo aver presentato una vasta gamma di infezioni digitali ed aver effettuato delle opportune distinzioni tra un tipo di virus ed un altro, il virus ci ha dimostrato come esso possa **influenzare l'arte digitale; sia fonte d'ispirazione per l'arte e esso stesso oggetto d'arte digitale applicata**, degno quindi di stare all'interno di un museo. Ci ha svelato il suo potenziale artistico, il suo potere

DIGITALCRAFT # HAUS DER KULTUREN DER WELT

[31 gennaio - 6 febbraio - Berlino]
Oltre a Digitalcraft, ecco chi c'è dietro all'esposizione di quest'anno:
Transmediale - International Media Art Festival Berlin
www.transmediale.de
Haus der Kulturen der Welt
www.hkw.de

VIRUS IN MOSTRA

Si sa che un museo raccoglie, classifica e conserva collezioni di oggetti rilevanti dal punto di vista storico, tecnico, scientifico ed artistico. Nel contempo però, come spiega Franziska Nori responsabile dell'esposizione di Berlino, il museo è anche un laboratorio, serve a comunicare e ricercare nuove realtà. E come infatti Digitalcraft è interessata da un lato alle nuove forme di produzione tecnica; dall'altro è un'area di ricerca e di riflessione sulle nuove tecnologie e il valore che esse assumono nella società dell'informazione e per l'arte. Ma non è l'unica! Qui di seguito quando, dove e ad opera di chi i virus sono entrati nelle mostre, nei musei e addirittura nelle università.

EL CUERPO DEL ARTE

[2001 - Biennale di Valencia]
Alla mostra El Cuerpo del Arte (sezione El Mundo Nuevo), una delle principali manifestazioni della Biennale di Valencia, gli epidemiC presentano il virus HTML.Reality.
www.epidemic.ws/valencia_press/el_pais.htm

I VIRUS COME FORMA DI ESPRESSIONE ARTISTICA

DIGITALCRAFT # MAK.FRANKFURT
[23 maggio 2002 – Francoforte]
Digitalcraft - Arts and Crafts in the Digital Age (Arti e Mestieri nell'Età Digitale) è una sorta di archivio della cultura digitale, un progetto e allo stesso tempo una sezione del mak.Frankfurt, Museum of Applied Arts Frankfurt (Museo di Arti Applicate di Francoforte), che già nel maggio 2002 concepì la prima esposizione all'interno di un museo dedicata al fenomeno dei computer, dal nome appunto I love you - computer_virus_hacker_culture.
www.digitalcraft.org
www.mak.frankfurt.de

estetico ed anche la sua capacità di raccogliere, produrre e diffondere informazione.

I love you, hacker culture!

Arte, estetica, sicurezza e tecnologia: questi i temi affrontati a Berlino. Nel museo allestito con vari terminali e **un database interattivo contenente centinaia di virus emulati** sono intervenuti net.artisti, programmatori, esperti della sicurezza IT, poeti del codice sorgente, sociologi e storici dell'arte. Sono stati affrontati la storia dei virus software e il loro sviluppo tecnico; sono stati resi visibili quei processi digitali e virali normalmente nascosti nella scatola nera del computer. **Il virus finalmente non più cosa oscura, ma addirittura manipolabile dai visitatori** i quali non solo hanno assistito a varie dimostrazioni di effetti e di interessanti payloads, ma hanno potuto attivare alcuni virus ed effettuare crash di sistema. Particolare attenzione è stata rivolta al **potere artistico dei virus**, all'intero processo creativo che porta alla loro realizzazione e in particolare all'estetica del codice e alla sua scrittura come atto estetico e nel contempo rivoluzionario. A rappresentare quest'altro volto del virus anche programmatori ed artisti italiani: gli **EpidemiC e i 0100101110101101.ORG, con i loro virus "biennale.py" e "bocconi.vbs"**, ormai dichiarati vere e proprie opere d'arte; e **Jaromil programmatore free software nonché artista**, i cui lavori hanno introdotto all'etica hacker e alla funzione estetica dei virus software. Per l'occasione è stato anche invitato Trend Micro, un produttore di software anti-virus più interessato al fenomeno dal punto di vista dell'economia e della sicurezza.

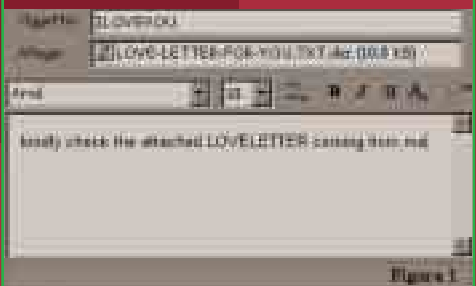


Figura 1



Non solo malattia

Il virus è apparso non solo come un agente patogeno, emissario del danno, ma come prodotto di un approccio sperimentale al linguaggio che è ancora in via di sviluppo; il codice o meglio il viruscode, permette al coder di creare programmi eseguibili che trascendono le funzioni canoniche, come lo stabilire una comunicazione tra chi lo utilizza (user) e il computer. **Il viruscode è infatti anche un testo con una sua estetica**, con una sua forma quale può averla qualsiasi linguaggio scritto e parlato. Nel codice, secondo gli epidemiC, "forma e funzione coincidono e raggiungono le altezze della poesia stessa con tutto il potenziale di un linguaggio che nasce per il net e si diffonde in esso". Per i programmatori consapevoli dell'infinita magia della loro arte, **i virus non sono dei semplici tool ma programmi di creazione artistica e il codice è una forma di poesia comparabile a quella sperimentale dell'ultima avanguardia** - Boudelaire, Rimbaud, Apollinaire e i surrealisti - alla poesia moderna di Jandl nella quale risalta la musicalità della parola, e il senso del dettaglio. Il codice, insomma, come testo da recitare (gli epidemiC **hanno recitato quello di I Love You**) o un Calligramma di Apollinaire che, ricordiamo, riusciva a dare forme grafiche diverse alle parole, rendendo la poesia disegno; come poesia concreta i cui testi ridotti a poche parole, lettere e segni di punteggiatura, aspirano allo status di oggetti d'uso o ad essere comprensibili in tutto il mondo, proprio come i cartelli stradali. Persino come **un haiku giapponese**, breve componimento di 5-7-5 sillabe privo di titolo, minimalista, asciutto e compatto, nel quale il poeta è solo uno strumento, mentre il soggetto è rappresentato dall'oggetto che anima il componimento. Nella forma di un haiku è **la prima poesia scritta in Perl da Lerry Wall nel 1990**. Nella poesia Perl che è program code e il program code è poesia, il testo può rappresentare l'ispirazione di chi lo ha scritto, adempiendo nel contempo, attraverso l'interazione col computer che l'interpreta, allo scopo per il quale è stato programmato. Così appaiono le opere perl di Sharon Hopkins ed anche i codeworks di A. Sondheim, programmatore ed artista, per il quale i virus sono stati appunto fonte d'ispirazione.

DaMe`
www.dvara.net/HK

UNIVERSITA' BOCCONI
[2002 – Milano]
Per recuperare i valori semantici e pragmatici originari di un termine (virus) che significa forza, vigore, nell'ateneo milanese il collettivo EpidemiC presenta il virus bocconi.vbs. Il contagio selettivo trasforma il possesso di questo Brand Virus in una questione di status: una provocazione lanciata proprio a partire dal centro nevralgico delle ricerche sulla brand image e sulla comunicazione aziendale.
www.epidemic.ws/bocconi/index_it.html

RISVOLTI TECNOLOGICI DELLA POSSIBILE GUERRA ALL'IRAQ



Dalla Rete mi guardi IDDIO, che a Saddam ci penso IO

Bush spamma i militari iracheni, prepara le mosse per la cyber guerra e avverte gli hacker patriottici: "non mettetevi in mezzo, e lasciate giocare noi coi server di Saddam".

Immaginate Saddam Hussein nel suo palazzo, mentre smanetta allegramente col suo portatile, **magari facendo shopping su Uranium Online** (che, tra l'altro, esiste davvero e ha come slogan <<La soluzione di ecommerce per il combustibile nucleare>). Ora immaginate che tutto a un tratto **il suo computer esploda di email**. Tutto Spam "made in USA"; migliaia di offerte. Prestiti senza garanzie; guadagna lavorando da casa; ingrandisci il tuo pisello... Sarebbe l'equivalente di un bombardamento informatico a tappeto, e Saddam si arrenderebbe nel giro di giorni".
Così scherza, **se c'è da scherzare su questo argomento**, Kevin Maney del quotidiano Usa Today.
Ma dice almeno due verità. La prima, è che **il Pentagono ha effettivamente una struttura**, chiamata Computer Network Operations (CNO), per l'attacco e la difesa sulla Rete. L'altra è che in effetti **il primo attacco informatico realizzato dagli USA ai danni dell'Iraq, è stato costituito da migliaia di messaggi email** indirizzati ai vertici militari, con un invito a ribellarsi al regime di Saddam e un vero e proprio manuale su come disertare. La prima arma elettronica è quindi proprio lo spamming.

>> Non solo spam

Ovviamente i piani per la guerra elettronica degli USA non si limitano allo spam, anche se ovviamente non se ne conoscono i dettagli. Molte speculazioni sono state fatte dopo la notizia che **Bush ha già approvato i piani per la cyberguerra**, ma anche chi voleva far credere si saperla lunga (come l'azienda di sicurezza mi2g), messa alle strette non ha saputo dire molto più di "Mah, ci potrebbero essere degli infiltrati che, a comando, staccano i centralini telefonici". Visto anche quello che è accaduto durante la guerra in Bosnia, dove sono state impiegate bombe in grado di bloccare le infrastrutture di comunicazione in un raggio molto largo, **ci si aspetta qualcosa di più dai geek del Pentagono**.

>> No agli hacker patriottici

Un documento del centro nazionale per la protezione delle infrastrutture (NIPC) avverte che molto spesso, **in caso di guerra, gli attacchi ai sistemi informatici tendono ad aumentare** (www.nipc.gov/warnings/advisories/2003/03-002.htm). Non si tratterebbe tanto di attacchi organizzati dal diretto nemico degli USA (l'Iraq), ma soprattutto una risposta da parte di singoli cittadini e organizzazioni, domestiche o straniere, **che vogliono in qualche modo contribuire alla causa** realizzando intrusioni in sistemi collegati all'una o all'altra parte.
In particolare, il NIPC cerca di mettere in guardia i cosiddetti "hacker patriottici", che potrebbero attaccare obiettivi iracheni (o filo-iracheni) o di associazioni contro la guerra. A tutti loro, manda a dire che **l'amministrazione non condonerà alcuna attività illegale**, che verrà perseguita e punita indipendentemente dalle motivazioni patriottiche che l'hanno ispirata.
Un altro aspetto dell'avvertimento fa un po' sorridere, perché più che agli hacker sembra indirizzato a **script kiddies un po' pasticcioni**. Secondo il NIPC infatti c'è il rischio che qualcuno possa ingannare gli attivisti telematici fornendo loro degli strumenti di attacco che dichiarano di colpire obiettivi iracheni, ma che in realtà **puntano in effetti a siti americani**. E se si spingono a dire certe cose, probabilmente è perché è davvero successo...

CONTINUIAMO A ESPLORARE LE RETI P2P E I CLIENT PIÙ DIFFUSI

UN ORSO SERVIZIEVOLE

BearShare è il client più diffuso fra quelli che si avvalgono del noto protocollo Gnutella: solido e gradevole nell'interfaccia, dispone di una base di utenti decisamente ampia, fra cui moltissimi italiani.

Gnutella: un nome allettante per un protocollo che ha rappresentato una svolta decisa nella breve ma intensa storia del peer to peer. Si parla dei tempi del declino del glorioso Napster: i programmatori di Nullsoft, per intenderci i "genitori" di WinAmp, si misero a pensare a qualcosa che potesse degnamente sostituirlo, possibilmente **senza averne le limitazioni (né quindi condividerne i rischi)**. Nacque così Gnutella, e riuscì così bene che Aol, proprietaria di NullSoft, **ne bloccò subito lo sviluppo**, col timore che potesse diventare davvero un Napster migliore e più inafferrabile, e che disturbasse un po' troppo gli interessi delle major discografiche in cui la stessa Aol aveva compartecipazioni (vi dice niente il nome Time Warner?). **Ma ormai il seme era germogliato, e in molti lavorarono a client che supportavano questo nuovo protocollo**, implementandolo e migliorandolo.



>> Come funziona Gnutella

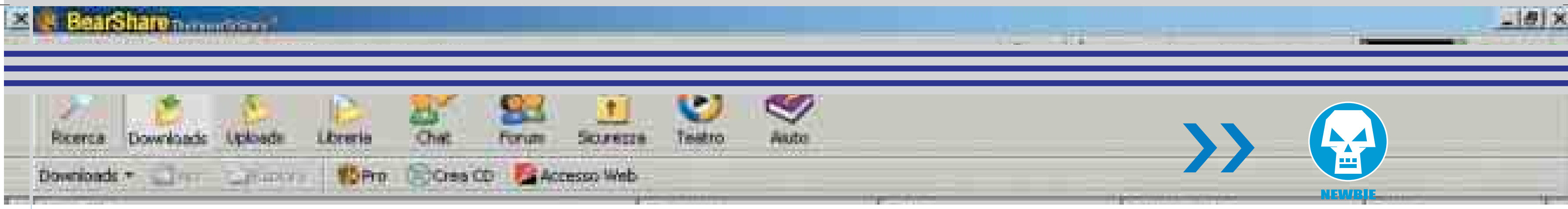
Il funzionamento di una rete Gnutella è semplice: **non esistono server centralizzati**, ogni utente è "servent" (server e client al tempo stesso). Quando un servent entra in rete, comunica la sua presenza a un altro servent, che già a sua volta avrà comunicato la sua presenza ad altri, in successione lineare, e che comunicherà a sua volta l'arrivo del nuovo servent, sempre nella stessa successione. Per fare un esempio pratico, il computer A, arrivando in rete, comunicherà la sua presenza a B, che avrà già comunicato a C la propria presenza, al suo ingresso in rete, e che ora farà la stessa cosa con A. C a sua volta comunica la presenza di A e B a D, e via dicendo. **Il numero di servent che "si parlano" è limitato dal Time To Live dei messaggi**, ovvero di passaggi che il messaggio compie sulla rete, che è limitato per evitare saturazioni della rete. A questo punto i computer così interconnessi potranno ricercare reciprocamente fra i file messi in condivisione.

? **Time To Live:** per evitare che il computer rimanga in attesa per sempre, le richieste in rete hanno spesso un "tempo di scadenza", trascorso il quale verranno ingorate.

>> Installare BearShare

In fase di installazione, la prima cosa che ci colpisce è il bonario annuncio che ci avverte che **BearShare è "sponsorizzato", ovvero contiene uno spyware**, Save! e ci invita a localizzarci, ovvero indicare la nostra posizione geografica, per usufruire del servizio di previsioni WeatherCast. Per il resto, l'installazione procede regolarmente, e al termine della stessa ha inizio la proceduta guidata per l'inserimento dei parametri di configurazione. La prima finestra sottende al **comportamento generale del programma**: modalità di chiusura e minimizzazione, esecuzione o meno all'avvio di Windows, visualizzazione delle anteprime e applicazione dei filtri (per contenuti "per adulti" e genericamente per







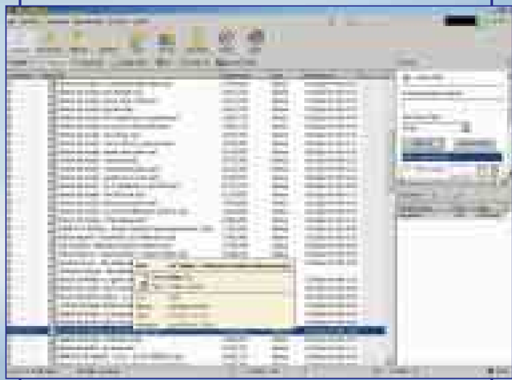
tutti i contenuti visuali, ovvero immagini e video). Quindi la scelta del tipo di connessione di rete, della posizione delle cartelle e la ricerca di file e cartelle condivisibili, come avviene per un po' tutti i client peer to peer.

>> Utilizzare BearShare

In fase di installazione, come già visto, vengono create due cartelle, una per i download, uno per i file temporanei (download non completati). Queste cartelle sono esplorabili mediante il menu File. Ma **per esplorarle bisogna prima riempirle...** vediamo come cominciare. Le voci di menu sono semplici e pressoché autoesplicative: Ricerca, Downloads, Uploads, Libreria, Chat, Forum, Sicurezza, Teatro e Aiuto. Ricerca ha un'interfaccia simile a quella della funzione Trova… di Windows. Oltre che indicare le parole chiave, **si possono selezionare i file per dimensione minima e massima, tipologia, e utilizzare un filtro antispam** per escludere dalla ricerca i file con nomi troppo lunghi o contenenti parole troppo lunghe. Un doppio clic sui risultati di nostro interesse basterà ad avviare il download.
In Downloads e Uploads si può controllare lo stato dei file in scaricamento e in prelievo da parte di altri utenti. Un clic destro su file permetterà di intervenire su di essi, sospendendo o interrompendo l'operazione o cercando altre fonti da cui scaricare lo stesso file.



Libreria visualizza i file ordinati per tipo, condizione (condivisi o meno), isolando i duplicati.
Chat e Forum danno accesso rispettivamente ai canali di chat e al forum ufficiale di BearShare, per comunicare con gli altri utenti e trovare risposte ad eventuali dubbi. In Sicurezza si può effettuare un **controllo antivirus sui file scaricati** mediante lo strumento FreeScan di McAfee.
Teatro mostra l'anteprima dei file video in scaricamento (per quei tipi di file che consentono tale operazione).
Aiuto dà l'accesso alla guida in linea di BearShare.



Questo è tutto quello che basta per utilizzare con soddisfazione BearShare. Ma è opportuno, ad ogni buon conto, fare ancora qualche cenno sulla configurazione avanzata. Nella voce di menu Impostazioni, troviamo le voci Condivisione, in cui si possono selezionare le cartelle da condividere, Ricerca, dove si possono determinare il numero di risultati, di upload e download contemporanei, limitare la banda utilizzabile, indicare i percorsi delle cartelle per download e file temporanei, oltre che intervenire sui valori indicati in fase di setup per modificarli. **Sono presenti anche configurazioni avanzate su servizi e autenticazione**, per chi volesse davvero mettersi al sicuro.

>> Altri client Gnutella

Ci sono **diversi altri client che si basano sul protocollo Gnutella**, e che quindi possono condividerne la rete: fra questi, ricordiamo Gnucleus (www.gnucleus.it, opensource per Win-



dows), GTK-Gnutella (http://gtk-gnutella.sourceforge.net, GPL per Linux) e LimeWire (www.limewire.com, opensource (ma non GPL) in Java, operativo su tutte le piattaforme, incluso Mac e Linux). Quest'ultimo, in particolar modo, è il "rivale" più importante di BearShare, potendo far affidamento prima di tutto sulla sua struttura in Java, completamente interpiattaforma, nonchè su una interfaccia forse ancora più seducente di quella di BearShare.

Paola Tigrino

SPYWARE E PRIVACY

BearShare ci pone davanti a una scelta: o ne acquistiamo la versione Pro (a 19 dollari e 95, non una cifra stratosferica, in effetti) o utilizziamo la versione gratuita, che porta con sé in bundle, senza possibilità di scelta, Save!, e WeatherCast. Save! è uno spyware. Nessuno prova neppure a nasconderlo, e in effetti è presentato un po' come gli spot pubblicitari alla televisione: volete il programma? Sorbitevi questi. E di tanto in tanto appaiono bannerini pubblicitari a tradimento, Il concetto non fa una piega, se non fosse che questi programmi si dimostrano un po' invadenti in fatto di banda e risorse di sistema, provocando rallentamenti e crash, e persistendo (nel caso di Save!, visto che in effetti WeatherCast ha un proprio uninstaller) anche dopo la disinstallazione di BearShare. Fatti salvi quindi i principi di "pagare un prezzo" per l'utilizzo di un software, è bene sapere come liberarsi di Save!, prima o poi.
La cosa migliore da fare è utilizzare un software come Ad-Aware (www.lavasoft.nu), che permette di individuare e rimuovere tutti gli spyware presenti, o altrimenti (ma perché rischiare?) andare pazientemente a caccia, nel disco e nel registro, di tutte le tracce di questo invadente adware/trackware (è questa, tecnicamente parlando, la sua categoria).

DIFENDERE IL PROPRIO COMPUTER DA INTRUSIONI NON AUTORIZZATE



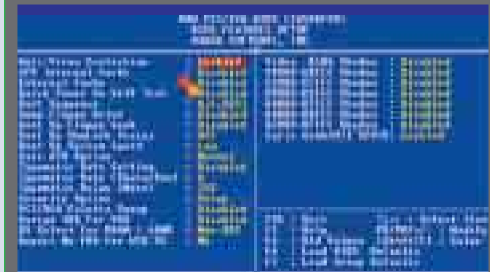
GIÙ LE MANI

Pensate che la password del salvaschermo basti a fermare un malintenzionato? Questo articolo vi farà cambiare idea...

Tanti di voi sapranno usare un firewall, avranno un ottimo anti-virus sempre aggiornato e probabilmente proteggono il loro PC da una password lunghissima e magari che credete impossibile da violare. Sfortunatamente, **ci sono dei metodi per superare senza troppa difficoltà la famigliare schermata di Windows che richiede la password** per il Nome Utente Giorgio (per esempio).
Bene, in questo articolo vedremo **alcuni dei potenziali problemi di sicurezza presenti in Windows 95, 98, XP, Me, 2000** e probabilmente tutti i sistemi operativi della Microsoft che possono essere usati per ottenere un accesso illegale a un computer da locale. Vediamo alcune situazioni tipiche…
Possibile situazione: scuola di un istituto che ha un normalissimo laboratorio di informatica e tanti bei computer collegati insieme in una rete. Normalmente, per uso scolastico e casalingo vengono installati sulle macchine dei sistemi operativi Windows. Nel nostro caso sarà la versione 98. Quando si accende il computer principale, che chiameremo SERVER viene chiesta una password per il nome utente SERVER. Ciò che voglio dimostrare è semplicemente la facilità con cui si può ottenere un accesso e per farlo sarà necessario trovare una password.
Esistono tre facili espedienti che potrebbe usare un cracker per riuscire nell'intento.

>> Boot alternativi

Quando un computer viene avviato il BIOS cerca un dischetto di boot oppure un CD di boot (dipende da come è settato il BIOS). **Chiunque quindi potrebbe entrare procurandosi un dischetto di boot** (per dischetto di boot si intende il floppy di avvio dell'installazione di Windows 9x, o un altro dischetto contenente un sistema avviabile) di Windows98 o 95 e inserirlo nel lettore. Quando il BIOS lo leggerà, verrà chiesto ciò che si intende fare e selezionando il prompt dei comandi verrà fornita una shell di DOS pronta per essere utilizzata e **con cui si può fare di tutto**.
Per evitare che qualcuno agisca in questa maniera, è sufficiente cliccare il tasto CANC all'avvio del PC e **settare il BIOS in maniera che non legga i floppy di Boot**, completando il tutto con l'assegnazione di una password per poter entrare nella configurazione del Bios. Le operazioni da compiere cambiano a seconda della scheda madre utilizzata, ma normalmente trovate un'opzione "Set password" nelle opzioni "Bios features".
Naturalmente **non siete ancora sicuri**. Avete solo diminuito un po' il rischio. Infatti, il computer potrebbe anche andare a cercare un CD di boot e se il cracker ne avesse uno saremmo al punto di prima, quindi bisogna ricordarsi di **eliminare anche la ricerca di un sistema dal CD-ROM**. Questa opzione si trova di solito alla voce "Boot sequence" nella finestrea "Standard features" delle impostazioni del bios della scheda madre.
Avendo settato la password per il Bios sarete sicuri che nessuno possa entrare nella modalità di configurazione. Per farlo bisognerebbe craccare la password e sarebbe necessario lanciare un programma che naturalmente l'hacker non potrà eseguire senza essere entrato in Windows o aver ottenuto una shell.
Sfortunatamente ci sono altri metodi più complicati che possono essere adoperati per scopi maliziosi.



La schermata del bios dalla quale si può decidere di escludere alcuni tipi di disco dalla ricerca di un sistema avviabile. Se si seleziona solo il disco C, sarà impossibile accedere al computer usando un floppy o un CD di sistema.

DAL MIO PC!

Purtroppo esiste ancora un modo per violare il vostro PC, anche se è molto più complesso.



Modificando il file msdos.sys si può impedire che un malintenzionato effettui il boot in modalità MS-DOS all'avvio di Windows.



Provocando un errore durante l'avvio di Windows, si avrà accesso al menu che permette di riavviare in modalità provvisoria o con una shell di MS DOS.

>> Evitare l'avvio di Windows

Se all'avvio del PC vi è mai capitato di cliccare il tasto F8 avreste fatto una utile scoperta...
Provate e vi ritroverete davanti a una schermata che chiede istruzioni su cosa desiderate fare; ci sono numerose opzioni: avvio in modalità provvisoria, con supporto di rete, ma quello che interessa a noi è **"prompt dei comandi in modalità provvisoria". Selezionate quello e potrete usufruire della comoda shell di DOS.**
Ora, pensate che chiunque potrebbe fare ciò che voi avete appena fatto e capirete che anche senza la vostra password avrebbe accesso al vostro caro computer.
Per evitare che succeda, basterà editare il file C:\msdos.sys. Alla voce [Options] modificate BootKeys=1 con BootKeys=0 (in caso non ci sia la riga BootKeys=1, createla voi). Fate attenzione al fatto che msdos.sys è un file normalmente invisibile, per cui sarà necessario attivare la visualizzazione di tutti i file dal menu Visualizza/Opzioni Cartella/Visualizza.

>> Provocare un errore

Se Windows non si avvia con successo, quando viene avviato nuovamente mostrerà una schermata di allarme che dice approssimativamente così: "Non si è riusciti ad avviare Windows. Si consiglia di riprovare in modalità provvisoria".
E' la stessa che appare quando viene cliccato F8! Allora basterà selezionare "prompt dei comandi..." per ottenere una shell di DOS. Questo ultimo baco è una misura di sicurezza di Windows e non vi conviene cercare di disattivarlo. Per far sì che Windows non si avvii correttamente **basta spegnere il computer durante la procedura di avvio**, dopo che è comparso il logo di Windows. In questo modo, si potrà accedere alla schermata di avviso!
Comunque, se volete cercare di bloccare anche questo tentativo di attacco, basterà editate sempre il file C:\msdos.sys, stavolta inserendo la riga BootFileSafe=0 sempre nella sezione [Options]. **Questo non è però consigliato, poiché in caso di qualche errore non potrete riavviare il PC in modalità provvisoria** creandovi un bel po' di guai.

>> Furto di password

Ma perché qualcuno dovrebbe cercare di ottenere una shell di DOS? Il motivo è semplice: **se un malintenzionato digitasse "format C: "** (comando che serve a cancellare l'intero contenuto del disco rigido) potrete pure cominciare a piangere.
Oppure potrebbe copiare su A: il file delle password. Si tratta di file con estensione .pwl e che si trovano in C:\Windows per quanto riguarda Windows 9x.
Quindi non dovrebbe far altro che inserire un floppy e digitare:

```
copy C:\Windows\*.pwl A:
```

Il comando copierà tutti i file con estensione *.pwl nel floppy.
Una volta arrivato sul proprio computer, troverà il file *.pwl che corrisponde all'utente SERVER. In questo caso è chiaro che il file sarà SERVER.pwl, perché il nome ha 5 caratteri. In caso ne avesse più di 8, allora verrà troncato all'ottava lettera. Per esempio ad un utente chiamato Massimiliano corrisponderà un file chiamato Massimil.pwl. Il file è cifrato, ma su Internet i programmi in grado di decifrarlo sono diffusi come le teenager russe disinibite.

witch_blade

Shell per il Mac OS tradizionale

Classicamente UNIX



Non è necessario avere il nuovo Mac OS X per poter impartire comandi a un Macintosh attraverso una linea di comando

Come abbiamo visto nel numero scorso, il sistema operativo attuale degli Apple Macintosh poggia le sue solide fondamenta su Unix, nello specifico su una variante di BSD denominata Darwin. MacOS X offre per la prima volta, oltre alle solite funzionalità dell'interfaccia grafica, anche una shell, una modalità di interazione a caratteri.

Tuttavia, contrariamente a quanto molti credono, **anche prima dell'arrivo OSX era possibile accedere alle risorse del Macintosh e impartire comandi in un ambiente puramente testuale**.



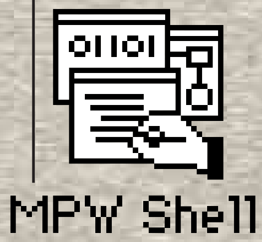
Le possibilità erano e sono molteplici e spaziano da ambienti di sviluppo a programmi appositi, spesso implementazioni di pezzi di Unix per Mac.

>> Per programmatori

Cominciamo da **MPW, Macintosh Programmer's Workshop** (http://developer.apple.com/tools/mpw-tools/), che è il framework di sviluppo ufficiale della Apple. Funziona su Mac OS 7.x/8.x/9.x ed è un ambiente aperto, configurabile e manipolabile tramite script con il supporto per vari linguaggi tra cui il C, C++ e l'assembly.

Riservato a lungo agli sviluppatori registrati con Apple dietro pagamento di diverse centinaia di dollari, **MPW è dal 1997 disponibile gratuitamente a tutti** via ftp all'indirizzo ftp://ftp.apple.com/developer/Tool_Chest/Core_Mac_OS_Tools/MPW_etc./

La parte che però più ci interessa è l'applicazione cuore, l'MPW Shell (ftp://ftp.apple.com/developer/Tool_Chest/Core_Mac_OS_Tools/MPW_etc./MPW-GM/MPW/MPW_Shell.sit.hqx) che a prima vista potrebbe venire confusa per un semplice programma di videoscrittura.



Digitando 'Help' ad inizio riga, seguito dal tasto Enter (l'Enter del tastierino numerico, non il classico tasto Return-Invio) **ci si trova dinanzi ad una successa lista di comandi**.

Quelli più direttamente utili alla manipolazione della macchina e del del filesystem sono raccolti sotto le categorie: **FileSystem, System e Launch**.

Troviamo comandi utili alla manipolazione di file e volumi (dischi, partizioni, etc.) come 'Files', corrispettivo di 'ls' in Unix o 'dir' in Windows, 'Move' ('mv'), 'NewFolder' ('mkdir'), 'Delete' ('rm' o 'del') e tanti altri tra cui 'Directory' ('pwd') che mostra il path, il percorso attuale in cui ci si trova, e svela anche una particolarità del filesystem Mac

```
Directory
Applicazioni:utilities:MPW:
```

i simboli separatori per le directory sono i due punti, ":" (invece che "/" e "\", slash e backslah).

Tra gli altri comandi interessanti da citare 'Volumes' per mostrare i dischi montati, 'Mount' e 'Unmount' per montarli e smontarli e 'Erase', per inizializzarli (formattarli), 'Shutdown' per spegnere o riavviare il computer e 'Launch' per controllare altri programmi (si può lanciare, fermare, stampare ed altro ancora).

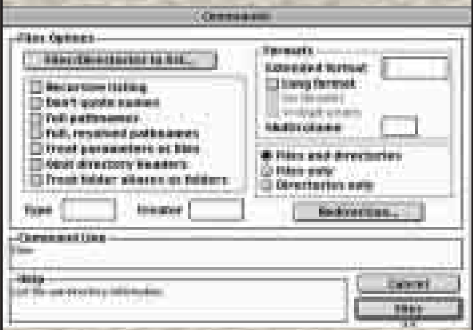
Da notare che **per eseguire il comando testuale abbiamo tre modi**: il già citato Enter del tastierino numerico, il classico tasto Invio insieme al tasto mela (command) o fare clic sulla barra in alto a sinistra sulla scritta 'MPW Shell' . Di default **i comandi NON sono case-sensitive** e la loro esecuzione può essere interrotta con la classica combinazione tasto mela+punto (command+".").

A ribadire che si tratta sempre di Macintosh, per molti comandi esiste una finestra di dialogo, detta "Commando" che permette di vedere e controllare più facilmente tutti i "flag", e che si invoca aggiungendo in più il tasto opzione (quello con la scritta "alt").

>> Classic Unix

Dopo MPW una citazione d'obbligo va ad **A/UX, il primo e sfortunato tentativo di Apple di creare uno Unix per il Macintosh**. A/UX fondeva l'ambiente Unix e la GUI del MacOS con risultati interessanti. A/UX purtroppo è tuttora a pagamento (anche se non più commercializzato) e **funziona solo su particolari vecchi modelli di Macintosh**. Inoltre A/UX è un sistema operativo completo che rimpiazza quello del Mac e quindi esula dalla nostra trattazione.

Esiste invece una serie di prodotti che è riuscita ad **implementare sopra il Finder una funzionale shell UNIX, in due casi addirittura con il supporto dello standard POSIX**, la Portable Operating System Interface (www.pasc.org/).



Il primo è **Mac06** (www.dsitri.de/projects/mac06/index.html), che funziona dalla versione 7 del MacOS ed offre un **ambiente di sviluppo in C**. Mac06, la cui pronuncia in inglese ("Mac oh six") richiama lo standard POSIX, è un kernel perfettamente funzionante che, oltre a permettere di usare comandi, scorrazzare per il filesystem, lanciare programmi grafici MacOS, dà anche accesso allo stack TCP/IP (e quindi al telnet, mail, ftp...).

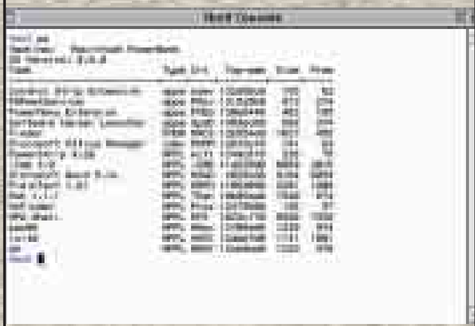
La curiosità di Mc06, e una dimostrazione della sua essenza Unix, è che quando è in funzione vengono lanciati in background anche due processi "initd" e "sh" che risultano visibili nel menù delle applicazioni di MacOS.

Il secondo tentativo è rappresentato da **LAMP** (http://lamp.sourceforge.net), acrostico ricorsivo che sta per "LAMP Ain't Mac POSIX" -LAMP non è Mac POSIX-, un ambizioso progetto ancora in-



completo che ha però una componente funzionante, Genie.

Genie (http://lamp.sourceforge.net/genie.html) fornisce una **shell ancora piuttosto limitata** con accesso ad alcuni comandi UNIX ed ha la particolarità di non usare i due punti ma il canonico "/", come si può vedere dando un banale 'pwd'.



```
$ pwd
/Volumes/Applicazioni/utilities/Genie.0.3.0/ e
```

Più ostica ma molto affascinante è **Msh** (http://my.vector.co.jp/servlet/System.FileDownload/download/http/0/31059/pack/mac/util/shell/Msh_1.1.1_f.sit.bin), una essenziale shell di tipo "csh".

L'uso di Msh è reso difficile dal fatto che **il programma è stato sviluppato da un giapponese** e di conseguenza tutti i manuali e gli help online (compreso il comando 'man') sono in questa lingua.

Mac Shell comunque offre svariati comandi tra cui 'cd', 'clear', 'pwd', 'ps', 'cat', 'cp', 'grep', 'ls', 'more', 'mv', 'rm', 'rmdir', il ridirezionamento dell'output e addirittura anche l'editor 'vi'.

In inglese, anche se forse un po' più limitato nelle funzionalità, è il programma **Mac Default Shell** (http://freaky.staticusers.net/macintosh/MacShell.0.54b.sit.hqx).

Anche qui si tratta di una "C shell": i comandi sono quelli tipici di Unix con qualche aggiunta, c'è un text editor e in più abbiamo un classico file di configurazione ("macshell.rc").

>> DOS e altro

Per la serie "stranezze" ecco invece **MacDOS 3.0** (http://wuarchive.wustl.edu/systems/mac/amug/files/util/m/macdos-3.0.sit.hqx).

Evidente già dal nome, MacDOS è un interprete di comandi che usa la sintassi dell'**MS-DOS Microsoft**, ha una lista impressionante di comandi tipici ('DIR', "CD", "TREE", "DEL", "COPY", "MD"...) e, colmo dell'ortodossia, **anche un file "autoexec.bat"**.

Finiamo con un "outsider" e più precisamente un editor di testo, **Plain Text** (http://hyperarchive.lcs.mit.edu/HyperArchive/Archive/dev/src/plain-text-121-c.hqx) che ha tra i suoi bonus un interprete di comandi testuali.

Come in MPW è necessario usare il tasto Enter alternativo (quello del tastierino numerico): comandi supportati sono quelli classici Unix come 'cat', 'cd', 'ls', 'pwd', più altri che compiono operazioni specifiche specifiche per il Macintosh.

Nicola D'Agostino
dagostino@nezmar.com

ESPLORIAMO I SERVER GRAFICI, I WINDOW MANAGER E I DESKTOP ENVIRONMENT

LE FINESTRE DEL PINGUINO



Se per Windows e Macintosh l'interfaccia a finestre è standard e scontata, su Unix le cose sono un po' più complicate...

Le passate versioni del sistema operativo MacOS, così come i componenti della famiglia Microsoft Windows dall'uscita di Win95 in poi, ci hanno abituato a pensare l'interfaccia grafica come una componente inscindibile dal resto del sistema operativo; tuttavia **la situazione sulla sponda Unix è decisamente differente**. L'interfaccia a finestre non è affatto parte integrante del kernel bensì è un normale processo e viene trattato come tale; inoltre possiede un'architettura fortemente modulare e, aspetto ancora più "innovativo", presenta **un'implementazione di tipo client-server**; vediamo però di andare con ordine...

L'X Window System (noto anche più semplicemente come X) nacque nei laboratori del MIT all'interno del più vasto Progetto Athena per lo sviluppo di un ambiente distribuito e verso la metà degli anni 80 comparvero già le prime VAX-workstation Unix della Digital con ambiente grafico X. L'origine del nome di questo sistema grafico, inzialmente svilpato da Robert Scheifler, Ron Newman e Jim Gettys e destinato in pochi anni a diventare lo standard de-facto per la grafica sotto *nix, è decisamente curioso; questi **nacque infatti allo scopo di sostituire W**, un precedente sistema di windowing sviluppato alla Stanford University, e pertanto **si scelse di utilizzare, in segno di continuità, la lettera successiva dell'alfabeto!**

In seguito venne creato nel 1998 l'X Consortium, un'associazione incaricata di promuovere e coordinare lo sviluppo di X e di diffonderlo sul maggior numero di piattaforme; tuttavia alcune divergenze portarono ad una biforcazione, e **nacque il progetto XFree86, i cui**

L'ambiente GNOME

Quando KDE fece la sua comparsa sulla scena Unix, molti furono gli utenti che si rifiutarono di supportare l'utilizzo delle librerie TrollTech per via della licenza proprietaria a cui erano soggette. Fu allora che il giovane Miguel de Icaza, noto all'intera comunità per aver creato mc - Midnight Commander, un clone avanzato del più diffuso Norton Commander per DOS, decise di dar vita ad un nuovo progetto per lo sviluppo di un Desktop Environment completamente libero; lo stesso Richard Stallman e il progetto GNU appoggiarono l'iniziativa e nacque così ufficialmente GNOME.



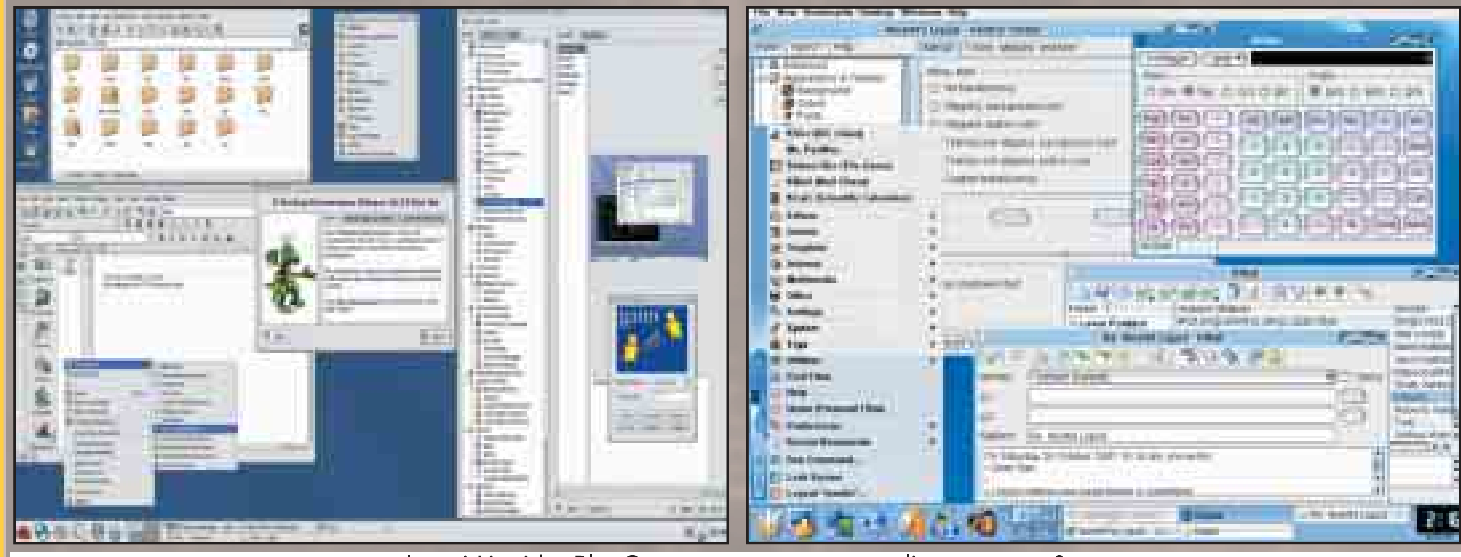
GIMP (GNU Image Manipulation Program) è un programma multipiattaforma nato originariamente per Linux e simile, se non superiore, per funzionalità ad Adobe Photoshop; per semplificare la realizzazione di questo programma gli autori crearono un apposito toolkit estremamente semplice ma potente e in grado di gestire la visualizzazione degli oggetti grafici (finestre, pulsanti etc..) chiamato appunto GTK (GIMP ToolKit+). Il progetto GNOME scelse proprio gtk+ come base per la creazione del nuovo ambiente e la maggior parte delle applicazioni sviluppate per GNOME si basano su questo kit di sviluppo, che conferisce al sistema un aspetto uniforme e consente ad esse di supportare correttamente i temi e i diversi wm.

Insieme alla Free Software Foundation, tra i sostenitori storici del progetto GNOME spicca RedHat Software, che quasi quattro anni fa decise di non utilizzare più KDE come desktop manager predefinito preferendo GNOME (anche se le prime versioni inserite si rivelarono eccessivamente instabili e immature). Nel 1999 la release 1.0 di GNOME venne finalmente alla luce e, sebbene TrollTech avesse in seguito modificato la licenza di QT optando per la GPL, lo sviluppo proseguì rapidamente e nel 2002 la versione 2.0 poté ad essere installata sui desktop di moltissimi utenti unix.

GNOME è l'acronimo di GNU Network Object Model Environment anche se lo stesso Miguel de Icaza sostiente di aver prima pensato ad un nome e di avergli solo in seguito dato un significato...

Il Tema è servito...

Ogni vero hacker ama personalizzare l'aspetto del sistema operativo su cui lavora in base al proprio gusto estetico; anche sotto Linux è possibile modificare in dettaglio il "Look 'n' Feel", l'aspetto dell'intero ambiente grafico: dall'immagine di sfondo alle combinazioni di colori delle finestre o dei pulsanti ed il loro comportamento, dai caratteri alle icone, gli splash screen (ovvero le schermate visualizzate all'avvio) o i suoni. Sotto Linux esistono infatti i cosiddetti "temi", ovvero dei file particolari che permettono di modificare in maniera semplice ed automatica l'intero aspetto del sistema. Esistono temi che vi faranno ad esempio dimenticare il freddo inverno con i loro colori caldi e rilassanti mentre altri si dimostreranno in grado di emulare, almeno nell'aspetto, l'interfaccia di altri sistemi operativi. Noti sono ad esempio i due temi per KDE Liquid e BlueCurve: il primo è in grado di competere ad armi pari con Mac OS X mentre il secondo, sviluppato da RedHat, ha come fine la creazione di ridurre al minimo le differenze tra GNOME e KDE offrendo agli utenti un GUI unificata.

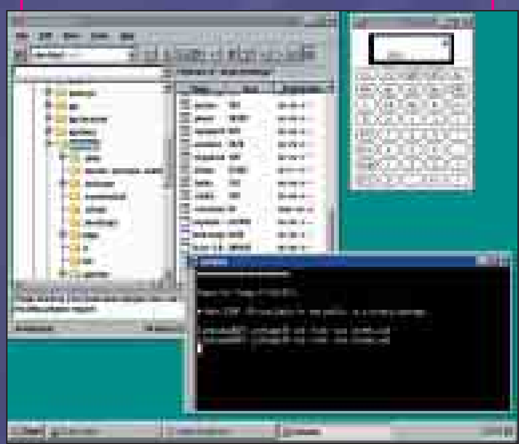


I temi Liquid e BlueCurve: veramente notevoli non trovate?

sforzi si diresso principalmente verso la piattaforma x86 (oggi molto diffusa ma fino ad allora "oscurata" dalle architetture RISC). Dopo una serie di vicissitudini, nel 1994 venne finalmente rilasciato XFree86 3.0 (basato sullo standard X11R6 del Consorzio); in seguito alcune restrizioni nei termini della licenza di X11R6.4, nel frattempo ceduto all'Open Group, spinsero però gli sviluppatori e il progetto XFree86 a "boicottare" l'Open Group. Da quel momento l'XFree86 divenne perciò il team di riferimento per lo sviluppo di X (non più solo su piattaforma x86) e, con la diffusione di Linux, la sua notorietà crebbe a dismisura.

>> Server e Client

L'idea fondamentale alla base dell'X Window System è quella di **fornire servizi minimi standard a programmi che visualizzano dati grafici**, utilizzando un display server in grado di gestire tutti i dettagli di interfacciamento. Lanciando solamente l'eseguibile di X sullo schermo appare una misera trama di sfondo e il cursore del mouse (solitamente un tozza croce): questo poiché il server X si occupa solamente della gestione di tutto ciò che permette di interagire con i diversi applicativi (schermo, tastiera e mouse, le componenti per l'appunto del display). Ogni altro software che funziona all'interno di una sessione X e **utilizza il server X per accedere a queste risorse**, ora visualizzando qualcosa sullo schermo, ora attendendo un input dall'utente, viene chiamato X client. Per riassumere, potremmo quindi affermare che il Server X funge da tramite fra le varie applicazioni/client che richiedono un output grafico su schermo e lo schermo stesso fisicamente inteso; le applicazioni infatti si limitano ad inviare le richieste al Server in maniera standard mentre **sarà compito del X Server gestire in maniera corretta l'hardware ed ottenere il risultato desiderato**. Inoltre questa struttura permette la visualizzazione grafica indifferentemente di applicazioni eseguite localmente o in remoto in maniera completamente trasparente; proprio niente male per un sistema progettato lustri or sono!



La variante in stile M$ del noto window manager Fvwm.

>> WM & DE...

..ovvero i **Window Manager (i gestori di finestre) e i Dekstop Environment (gli Ambienti desktop)**. L'aspetto che assumerà lo schermo del vostro computer dopo l'avvio di X Window dipenderà quasi interamente da voi: la gestione delle finestre, dalla decorazione alle modalità di acquisizione del 'focus', o i menu sono infatti gestiti direttamente da X bensì affidati al Window Manager. Moltissimi sono i WM disponibili per la vostra LinuxBox: twm, tra i primi ad apparire, **fvwm, semplice e leggero, AfterStep, WindowMaker e BlackBox, che emulano l'interfaccia di NeXT, o Enlightenment e Sawfish**, altamente configurabili e utilizzati con GNOME...
In seguito inoltre lo sviluppo della grafica sotto Unix ha spinto verso lo sviluppo di alcune soluzioni in grado di supportare quanto già altri sistemi operativi offrivano: in particolare la possibilità di disporre di un vero e proprio desktop ove poter sistemare icone e cartelle completo di taskbar. Al momento sono tre i principali ambienti di questo tipo disponibili sotto Linux: i due grandi avversari **GNOME e KDE** e il più compatto **XFce**.

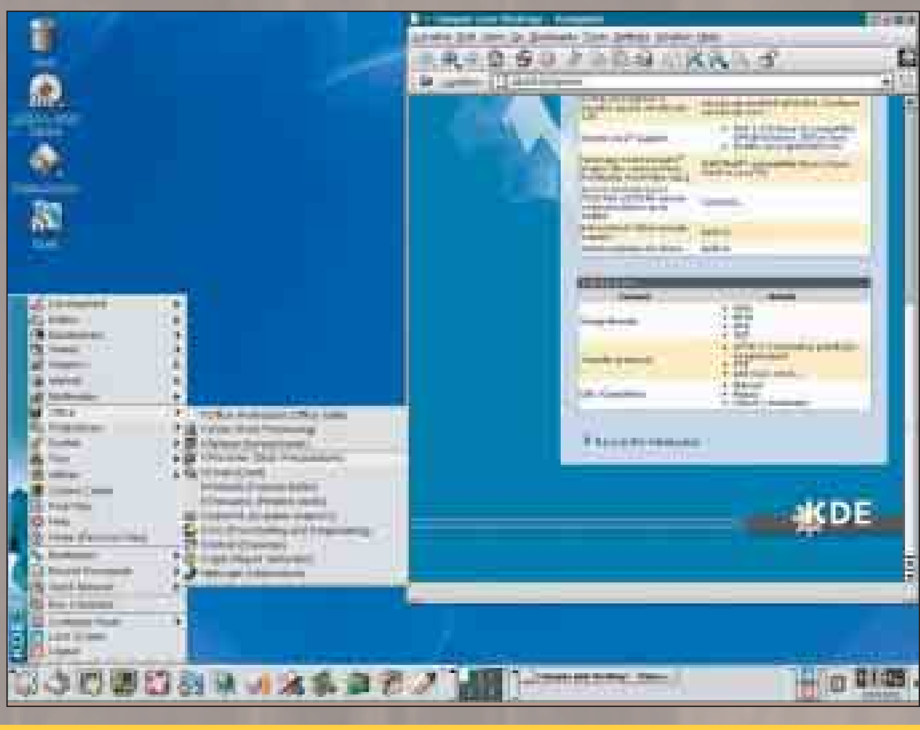
>> Non c'è 3 senza 4...

Nel Marzo 2000 il progetto XFree86 rilasciò ufficialmente la versione 4.0, che portava con sé numerose innovazioni. In particolare dalla versione 3.3.x alla 4.x **l'implementazione del server grafico è radicalmente mutata**: in precedenza infatti esistevano numerosi server, uno per ciascuna famiglia di chipset (ad esempio X8514 per le schede 8514, XS3 per le SiS S, XSVGA o XVG16 rispettivamente per le schede SuperVGA o VGA/EGA e così discorrendo) mentre, con la nuova major release, XFree86 è costituito da un unico eseguibile principale di base all'interno del quale possono essere caricati i moduli specifici per una particolare scheda. Per dovere di cronaca va segnalato che una tecnologia di questo tipo, simile per certi versi a quella che avevamo incontrato parlando del kernel Linux, è stata **inizialmente sviluppata dalla Metro Link e in seguito donata liberamente alla comunità dalla stessa**.

Lele - Altos.tk

Il desktop KDE

Tra il 1996 e il 1997 la TrollTech, una software house della fredda Norvegia, rilasciò la prima versione delle QT library, un widget per facilitare la programmazione in C++ sotto X. L'estrema semplicità e pulizia della programmazione in QT attirò numerosi programmatori e in particolare Matthias Ettrich, già autore di LyX, ne percepì immediatamente le potenzialità e decise di utilizzarle come base per un progetto estremamente ambizioso e dove in molti prima avevano fallito: realizzare un vero ambiente desktop per Unix. Attirati da quest'allettante prospettiva, sempre più persone iniziarono a contribuire al progetto KDE e lentamente furono resi diponibili i Kloni... ehm i cloni delle più diffuse applicazioni X11 esistenti (kless, kcalc, kdvi, kmail e così via). Con il successo, iniziarono però ad arrivare anche le critiche: per i tempi KDE era infatti troppo esigente in termini di memoria (32 Mb erano appena sufficienti per avere tempi di risposta decenti), troppo simile nell'interfaccia all'accerimo nemico MS Windows e, soprattutto, non libero! Le librerie QT infatti vennero inzialmente rilasciate sotto una licenza di tipo commerciale, lasciando però libertà di utilizzo per scopi non di lucro; questo fatto in particolare fece perdere il sonno ai membri della FSF e a molti sostenitori del software libero, nonostante TrollTech abbia in seguito optato per la più permissiva GNU GPL.
KDE 2, rilasciato alla fine del 2000, incluse inoltre KOffice, una suite di applicativi per l'office automation decisamente completa, e Konqueror, un browser/file manager/visualizzatore (effettua l'anteprima dei più disparati file multimediali) semplice ed estremamente performante; meno di un anno fa è stato infine rilasciato, migliorato ed ottimizzato per molti punti di vista, il nuovo KDE 3.
Curioso notare come la K di KDE non significhi nulla in particolare; in passato tuttavia, specialmente sui sistemi Unix proprietari, era diffuso un Desktop Manager chiamato, e non è solo un caso, CDE - Common Dekstop Environment (ovvero Ambiente Desktop Comune)...



INTRODUZIONE AL PROTOCOLLO TCP/IP

UNA QUESTIONE DI PROTOCOLLO

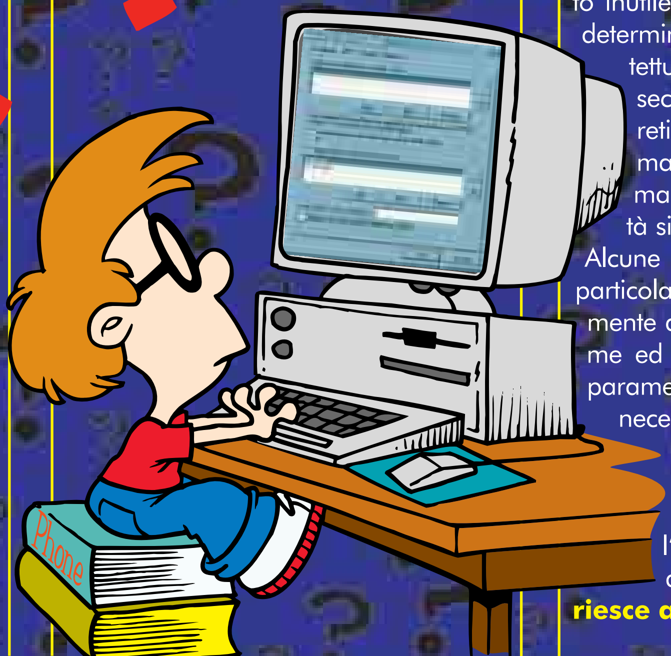
Quante volte l'avrete sentito nominare? "Setta i parametri TCP/IP, dammi il tuo IP", oppure in una pagina web la scritta: "il tuo IP è". Insomma, è un martellamento continuo... Ma cosa significano davvero queste sigle?

Partiamo un po' più da lontano e **vediamo innanzitutto cos'è il TCP/IP Internet Protocol suite**. Non è altro che l'insieme di due protocolli che interagiscono e che sono il **Transmission Control Protocol** e l'**Internet Protocol**.

Ma con la parola protocollo cosa diavolo intendiamo realmente? Dare una definizione scolastica sarebbe riduttivo e non chiarirebbe le idee, quindi vediamo una traduzione un po' meno letterale del concetto. Un protocollo è **una serie di regole che permettono ai messaggi in uscita da una macchina di raggiungere una macchina destinataria** ed essere da questa interpretati.

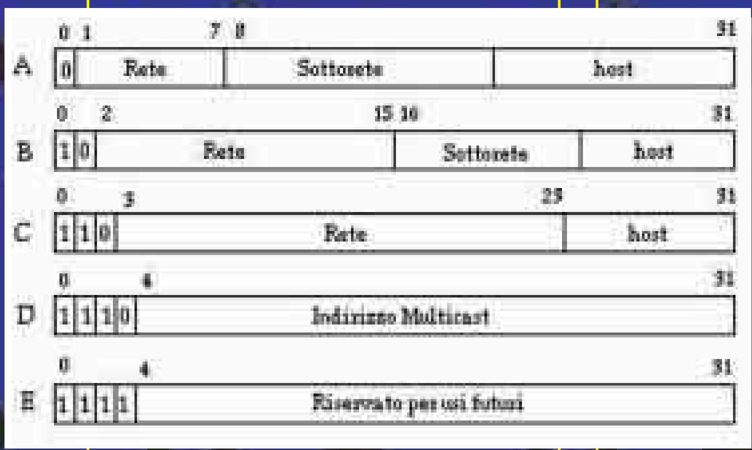
>> Com'è fatta Internet

L'architettura di Internet per la trasmissione dei dati è strutturata come un palazzo a più piani, dove ognuno di questi ha responsabilità ben precisa nella trasmissione del pacchetto. In pratica si può ipotizzare che dal piano più alto parta una busta, in quello inferiore qualcuno scriva l'indirizzo, al piano più basso ancora un altro affranchi la busta per poi passarla al piano terra dove il portiere la consegnerà al postino. Come si intuisce **è un lavoro concatenato dove non ci possiamo permettere di saltare nessun passaggio**.



Prima di analizzare l'architettura esatta dei pacchetti, cerchiamo di capire in maniera più approfondita come è strutturalmente organizzato Internet. Diciamo subito, a scanso di equivoci e per cancellare luoghi comuni, che **Internet non è una rete di comunicazione**, bensì l'insieme di innumerevoli reti di comunicazione. Questa che potrebbe sembrare una precisazione tanto inutile quanto banale, risulta invece determinante nel comprendere l'architettura stessa di Internet. Infatti, a seconda delle necessità, le varie reti dovranno essere strutturate in maniera specifica al loro utilizzo, ma ciò comporta un'ovvia diversità sia di hardware che di gestione. Alcune avranno necessità di essere particolarmente veloci, altre particolarmente affidabili, altre ancora sicurissime ed inattaccabili a scapito di altri parametri. Nasce proprio da qui la necessità di **implementare un protocollo che riesca ad "unire" tutte queste realtà**. La soluzione si avvale dell'Internetworking che, grazie a dei collegamenti detti gateway, **riesce a collegare reti totalmente**

diverse fra loro come se invece fossero strutturate tutte allo stesso modo. È a questo livello che si inserisce il TCP/IP che, grazie alle sue regole pubbliche, riesce in questo obiettivo.



>> Reti interconnesse

Ma come si attua l'interconnessione? Diciamo che lo stratagemma utilizzato è quello di **suddividere un determinato pacchetto in un certo numero di pacchetti molto più piccoli**, contenenti l'intestazione ed una certa mole di dati: il packet-switching.



Ma come avviene il trasferimento dei dati? Nell'introduzione di questo articolo ho detto che quando navighiamo online in pratica ci riduciamo ad una "misera serie di quattro triplette"; essa non è null'altro che l'IP, unico per ogni macchina e unico nella rete. È ovvio che se esistessero due PC aventi lo stesso nome sorgerebbero conflitti nella "consegna" dei dati.
La connessione fra macchine diverse avviene grazie a dispositivi responsabili del traghettamento dei vari pacchetti: i **routers**. Essi servono solo a far passare i dati da una parte all'altra della rete a cui sono connessi, ma devono anche sapere come far arrivare un determinato pacchetto in una zona di Internet con la quale loro stessi non hanno direttamente a che fare. Il router ragiona, quindi, per "reti", non curandosi dell'utente finale, ma cercando solo di far arrivare il pacchetto "in prossimità" di esso. Saranno poi altri sistemi a recapitarlo a destinazione. Per semplificare, si può immaginare un pacco che parta da casa mia per destinazione Mario Rossi, Via Roma 1, Firenze. Io porto il pacco al mio ufficio postale (1° router) che tramite corriere lo porta all'ufficio di Firenze (2° router); starà ora ai postini locali recapitarlo all'indirizzo esatto, ma in questo processo i routers non interagiscono più.
Vediamo quindi cosa sono e come sono strutturati effettivamente gli indirizzi IP. Sono **campi composti da 32 bit**;

> Datagramma IP
> Versione (4)
> L. header (4)
> Tipo di Servizio (8)
> Lunghezza totale (16)
> Identificatore (16)
> Flag (3)
> Offset del frammento(13)
> Tempo di durata (8)
> Protocollo (8)
> Checksum dell'header (16)
> Indirizzo IP origine (32)
> Indirizzo IP destinazione (32)
> Opzioni (Variabile)
> Riempimento (per allineare a 32 bit)
> DATI
> (Variabile, multiplo di 32 bit)

ne esistono cinque forme diverse, dette classi, determinate dai primi bit. Le prime tre classi **(A-B-C)** contengono l'indirizzo di rete a cui appartengono e l'indirizzo della macchina host, la classe **D** è utilizzata per il multicasting e la classe **E** è riservata ad impieghi futuri. Pur essendo di 32 bit, gli indirizzi IP si leggono a gruppi di 8 bit per volta (ottetto), per ovvia praticità, intervallati da punti (xxx.xxx.xxx.xxx). Le tre classi di IP vengono assegnate da un organo centrale e poi a livello locale i vari amministratori suddividono le numerazioni. I numeri di classe C sono attribuiti a reti di massimo 255 host, quelli di classe B fino a 65536 e quelli di classe A per reti di circa 16 milioni di host.

> **Multicasting** Trasmissione di dati che parte da una sola origine e viene inviata a più destinatari contemporaneamente, a differenza dell'Unicasting dove la comunicazione avviene da un computer ed è destinata a un altro soltanto.

Ma cosa succede quando devo spedire un pacchetto? Succede che io mando a tutti gli host di una determinata rete un pacchetto contenete i miei indirizzi (IP e fisico), i dati da spedire e la richiesta di recapitarli a quell'host specifico. Al momento della risposta ogni macchina aggiorna una propria tabella memorizzando così l'indirizzo fisico e l'indirizzo IP in modo da non dover compiere ripetitivamente questa azione che appesantirebbe in maniera inutile la rete.

>> Differenti livelli

Procediamo quindi nell'analisi di Internet e diciamo subito che essa è strutturata su tre livelli: **application services** (livello più alto che gestisce le applicazioni), **reliable stream transport service** (si occupa della comunicazione e delle sua affidabilità), **connectionless packet delivery service** (livello più basso che effettua la spedizione dei pacchetti). Proprio sul meccanismo IP si basa il livello più basso di questa torre. Si definisce come inaffidabile, senza connessione diretta e best-effort, ovvero al meglio delle possibilità; della serie... **il pacchetto parte, e cercheremo di fare del nostro meglio, sperando che arrivi!**
I pacchetti vengono gestiti come dei frame. Questi sono l'unità base del trasferimento dati e sono formati dall'header e dall'area dati.
Il datagram è un blocco di dati, un frame logico e come tale formato anch'es-



so da header e area dati. L'intestazione è molto complessa e vista nel dettaglio è divisibile come segue:

- i primi 4 bit contengono la versione del protocollo IP utilizzato
- i 4 successivi indicano la lunghezza dell'intestazione
- gli 8 seguenti indicano il tipo di servizio e la priorità del pacchetto
- i 16 successivi indicano la lunghezza totale del datagram.
- Segue poi il campo identificativo che serve a farlo riconoscere univocamente
- i 2 bit successivi entrano nel processo di frammentazione
- il terzo campo contiene la posizione dei dati nel blocco.

Il campo seguente indica la scadenza del pacchetto, si ha poi l'informazione sul protocollo di alto livello che ha generato i dati ed infine un campo di controllo per l'integrità dell'intestazione. In ultimo abbiamo i campi IP del mittente e del destinatario, seguiti da un campo contenete varie opzioni e da quello eventuale di riempimento.

>> Pacchetti in viaggio

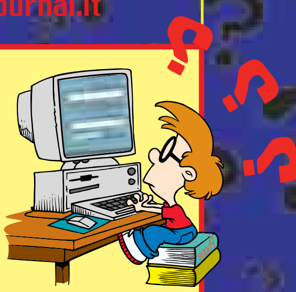
Come abbiamo detto in precedenza l'IP è un protocollo che **non presuppone connessione diretta tra due host che si scambiano i dati**, bensì una serie di connessioni variabili che portano il pacchetto a destinazione. La scelta della strada da percorrere è affidata ai router che, in base alla caratteristiche che la rete assume in un determinato momento, possono istradare un pacchetto in una direzione piuttosto che in un'altra. L'istradamento di un pacchetto può essere diretto, se l'host ricevente è nella stessa rete di quello trasmittente, o indiretto.

Tutta questa gestione best-effort dei pacchetti è affidata, come unico controllo, all'**Internet control message protocol (ICMP)**, che è considerato come parte integrante del protocollo IP stesso. Il datagram ICMP può contenere diversi campi, ma almeno tre sono sempre obbligatori, ovvero: identificativo del messaggio, il codice di errore, una somma di controllo. A essi si possono eventualmente associare altri parametri secondo quale codice di errore viene riportato.

Spero che questo articolo sia servito per chiarire le idee su come effettivamente un pacchetto che parte dal vostro PC possa raggiungere una qualunque parte della rete. L'articolo non pretende di essere esaustivo sull'argomento. Nel caso siate interessati ad approfondire maggiormente questa branca tecnica vi consiglio di perdere un po' di tempo online e cercare qualcuno degli innumerevoli documenti associati.

CAT4R4TTA
cat4r4tta@hackerjournal.it

Id	Tipo	Descrizione
0	Eco — risposta	Rimanda al mittente i dati che ha richiesto
3	Destinaz. non raggiungibile	Il gateway non ha spedito il datagramma al destinatario
4	Richiesta rallentamento	Chiede di ridurre la velocità di emissione dei pacchetti
5	Reinstradamento	Usato dai gateway per informare che esistono strade più efficienti
8	Echo — richiesta	Richiede al destinatario di rimandare i dati specificati
11	Tempo esaurito	Indica un datagram rimasto troppo tempo in rete senza raggiungere la destinazione
12	Errore parametrico	Utilizzato per i problemi non trattati da altri messaggi
13	Stampigliatura — richiesta	Utilizzato per la sincronizzazione di due orologi
14	Stampigliatura — risposta	Utilizzato per sincronizzare gli orologi di due computer
15	Informazioni — richiesta	Era utilizzato per risolvere il proprio IP
16	Informazioni — risposta	Era utilizzato per risolvere il proprio IP
17	Maschera — richiesta	Serve a chiedere quale parte dell'IP è la maschera di rete e quale l'indirizzo dell'host
18	Maschera — risposta	Serve a chiedere quale parte dell'IP è la maschera di rete e quale l'indirizzo dell'host



ANALIZZIAMO IL FUNZIONAMENTO DI UNO SNIFFER DI PACCHETTI

Ucci ucci... sento odor di pacchettucci!



Con qualche programma impostato bene, da un qualsiasi computer collegato a una rete, si possono intercettare e spiare le comunicazioni dirette a qualsiasi altra workstation della stesa rete.

Spesso l'azione di cracking viene identificata con il defacement di un sito. In realtà esistono azioni più pericolose che possono essere messe in atto da un eventuale intruso, una volta che sia riuscito a mettere le mani su almeno un computer di una rete remota. Non essendo altrettanto eclatanti della sostituzione della home page, queste azioni attirano di meno l'attenzione degli amministratori di sistema. **Stiamo parlando per esempio dello "sniffing"**, argomento di quest'articolo. Si tratta dell'arte di **"fiutare" informazioni da una rete**. Prerequisiti per seguirlo e utilizzarlo senza difficoltà sono una qualunque distribuzione linux e una certa conoscenza del C (variabili struct, cast eccetera). Per quanto riguarda le funzioni di libreria che gestiscono la connessione in rete necessaria per lo sniffing, cercheremo di descriverle in quest'articolo in modo da rendervele più 'digeribili'.



Prima di cominciare vorrei fare però una precisazione: **gli sniffer non sono soltanto strumenti d'attacco, ma possono aiutare molto gli amministratori di sistema** nella normale manutenzione della propria rete e probabilmente qualcuno di voi li avrà già utilizzati e conosciuti con il nome altisonante di analizzatori di pacchetti o di protocollo.

>> Principio di funzionamento degli sniffer

Quando, all'interno di una rete locale, un computer deve comunicare con un altro, crea dei pacchetti dati che contengono l'ip del computer destinatario. Questo avviene perché, in realtà, **il pacchetto viene inviato a tutti i computer della rete locale** giacché nei vari standard delle reti (stella, anello etc.) non vi sono collegamenti diretti tra un computer e l'altro. In pratica è come se l'insieme dei cavi, degli hub e degli switch di una rete si comportassero come un bus condiviso.
Come impostazione predefinita, le schede di rete presenti nei terminali e nelle workstation di una rete locale sono impostate



in modo tale da filtrare i dati che passano dalle loro parti, considerando soltanto quelli a loro diretti e scartando tutti gli altri. **Esiste però una modalità chiamata promiscua che consente di non scartare i dati diretti ad altre workstation** diverse dalla nostra e quindi di ascoltare gli scambi all'interno della rete locale, autenticazioni comprese. Vediamo adesso il sorgente di uno sniffer molto noto, linsniffer.c di Mike Edulla. Potete trovare la versione integrale al seguente indirizzo: http://www.dsinet.org/tools/network-sniffers/linsniffer.c. Se aprite il file con un qualunque editor di testo vi troverete di fronte, nella prima parte, alle seguenti istruzioni include:

```
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <netinet/in.h>
#include <netdb.h>
#include <string.h>
#include <linux/if.h>
#include <signal.h>
#include <stdio.h>
#include <arpa/inet.h>
#include <linux/socket.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/if_ether.h>
#include <sys/ioctl.h>
```

Questi include fanno riferimento ai file d'intestazione delle librerie utilizzate in questo programma. **E' importante assicurarsi di possederli tutti nella propria distribuzione Linux** alle cartelle /usr/include, /usr/include/net e /usr/include/netintet, altrimenti otterreste degli errori in fase di compilazione.

LE PRINCIPALI LIBRERIE

<linux/if.h>, contiene le definizioni per il controllo dell'interfaccia Ethernet. Potete trovarlo all'indirizzo: http://lxr.linux.no/source/include/linux/if.h

<linux/if_ether.h>, contiene le definizioni per l'interfaccia Ethernet IEEE 802.3 e gli altri protocolli Ethernet come AppleTalk (per la comunicazione con i mac) e Internet Protocol. Può essere consultato all'indirizzo: http://lxr.linux.no/source/include/linux/if_ether.h .

<linux/ip.h>, contiene le definizioni per l'implementazione del protocollo IP su Linux, consultabile all'indirizzo: http://lxr.linux.no/source/include/linux/ip.h .

<sys/socket.h>, la libreria cui fa riferimento questo file d'intestazione gestisce le operazioni del socket come listen, bind, connect, accept, send etc. Potete consultare anche questo file all'indirizzo: http://lxr.linux.no/source/include/linux/socket.h .

<linux/tcp.h>, Contiene le definizioni degli stati di connessione TCP come TCP_ESTABLISHED (connessione stabilita), TCP_LISTEN (in ascolto), TCP_CLOSE (in chiusura) etc. E' consultabile all'indirizzo: http://lxr.linux.no/source/include/linux/tcp.h .



Per analizzare il sorgente di Linux, potete consultare la versione ipertestuale del sorgente presente su internet all'indirizzo http://lxr.linux.no.
Tra i file d'intestazione precedenti vorrei segnalarvi quelli più utili alla nostra trattazione (vedi riquadro).
Dopo i file d'intestazione troviamo i prototipi delle funzioni implementate in linsniffer.c:

```
int openintf(char *);
int read_tcp(int);
int filter(void);
int print_header(void);
int print_data(int, char *);
char *hostlookup(unsigned long int);
void clear_victim(void);
      void cleanup(int);
```



Come potete vedere qui il codice è abbastanza chiaro: vengono definiti i nomi delle funzioni con il tipo dei parametri in ingresso e in uscita. Unica osservazione: nel prototipo char *hostlookup (unsigned long int), **l'asterisco non va con il nome della funzione**, perché in questo caso ci troveremmo di fronte ad un puntatore a funzione, bensì con char ossia la funzione hostlookup riceve in ingresso un intero lungo senza segno e restituisce un puntatore a carattere.
Dopo di ciò segue la dichiarazione delle variabili globali ossia quelle utilizzate da più di una funzione di linsniffer e che rimangono allocate in memoria per tutto il periodo in cui il programma è in esecuzione:

```
struct etherpacket
{
 struct ethhdr eth;
 struct iphdr  ip;
 struct tcphdr tcp;
 char buff[8192];
}ep;
```

Queste istruzioni dichiarano un tipo struct chiamato **etherpacket** e contemporaneamante creano una variabile del tipo etherpacket di nome **ep**. Vedremo in seguito qual è l'uso che ne viene fatto nel codice. Le definizioni dei tipi delle variabili struct **ethhdr, iphdr, tcphdr** sono contenute nel file d'intestazione **if_ether.h**.

```
struct
{
   unsigned long       saddr;
 unsigned long       daddr;
 unsigned short      sport;
 unsigned short      dport;
 int                  bytes_read;
 char                 active;
 time_t               start_time;
} victim;
```

Queste istruzioni dichiarano la variabile strutturata victim che conterrà i dati della comunicazione vittima come l'indirizzo e la porta del computer sorgente e destinazione, la quantità di byte letti il tempo di avvio (variabile del tipo time_t) e un char di nome active che fa dal flag.

```
struct iphdr   *ip;
struct tcphdr *tcp;
int s;
FILE *fp;

#define CAPTLEN 512
#define TIMEOUT 30
#define TCPLOG "test"
```

Queste ultime istruzioni della parte "dichiarativa"del codice non presentano particolari annotazioni: viene dichiarato il puntatore a file fp che servirà ad accedere al file di log in cui andranno inseriti i dati e vengono dichiarati due puntatori a variabili struct **iphdr** e **tcphdr**, che trovate definite rispettivamente in ip.h e tcp.h. In ultimo vengono definite le etichette CAPTLEN, TIMEOUT e TCPLOG con l'istruzione **#define**.

>> Analizziamo le funzioni

Cominciamo adesso ad analizzare le funzioni partendo naturalmente dalla funzione main:

```
main(int argc, char **argv)
{
 s=openintf("eth0");
 ip=(struct iphdr *)(((unsigned
                     long)&ep.ip)-2);
tcp=(struct tcphdr *)(((unsigned
                     long)&ep.tcp)-2);
 signal(SIGHUP, SIG_IGN);
 signal(SIGINT, cleanup);
 signal(SIGTERM, cleanup);
 signal(SIGKILL, cleanup);
 signal(SIGQUIT, cleanup);
if(argc == 2) fp=stdout;
 else fp=fopen(TCPLOG, "at");
 if(fp == NULL) { fprintf(stderr,
        "cant open log\n");exit(0);}
clear_victim();
 for(;;)
 {
     read_tcp(s);
      if(victim.active != 0)
print_data(htons(ip->tot_len)-sizeof(ep.ip)-
              sizeof(ep.tcp), ep.buff-2);
     fflush(fp);
 }
}
```

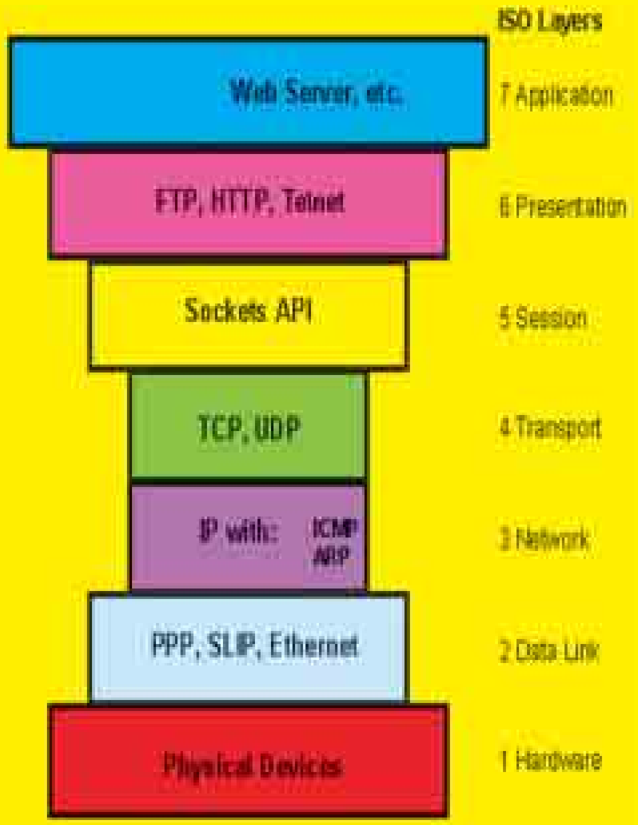
Per prima cosa, la funzione main cerca di aprire l'interfaccia di rete richiamando la funzione **openintf** implementata sempre in linsiffer.c. Questa funzione riceve in ingresso un puntatore ad una stringa di caratteri (nel nostro caso "eth0" cioè il nome dell'interfaccia) e restituisce un intero che fa da identificatore del socket creato. Vediamo in dettaglio come viene creato il socket analizzando il sorgente di openintf:



Socket: Un canale di comunicazione fra due processi su cui si possono leggere e scrivere dati attraverso la rete.
int openintf(char *d)

```
{
    int fd;
    struct ifreq ifr;
    int s;
    fd=socket(AF_INET, SOCK_PACKET,
htons(0x800));
    if(fd < 0)
    {
        perror("cant get SOCK_PACKET
                                 socket");
        exit(0);
    }
    strcpy(ifr.ifr_name, d);
    s=ioctl(fd, SIOCGIFFLAGS, &ifr);
    if(s < 0)
    {
        close(fd);
        perror("cant get flags");
        exit(0);
    }
    ifr.ifr_flags |= IFF_PROMISC; _- flag
di connessione promiscua
    s=ioctl(fd, SIOCSIFFLAGS, &ifr);
    if(s < 0) perror("cant set promiscuous
mode");
    return fd;
      }
```





Come potete vedere la quarta linea di codice richiama la funzione socket la quale riceve in ingresso tre parametri:

• il primo specifica il dominio del socket cioè la famiglia di protocolli cui deve appartenere il socket stesso: nel nostro caso AF_INET corrisponde alla famiglia di protocolli Ipv4.
• Il secondo parametro specifica il tipo di socket: nel nostro caso viene usato SOCKET_PACKET che è un tipo presente solo in linux e che consente di accedere al Data Link Layer (vedi la figura che rappresenta l'ip stack).
• Il terzo parametro indica il tipo di protocollo.

Questa funzione restituisce –1 se la creazione del socket non va a buon fine oppure un intero positivo che fa da file descriptor del socket (un po' come l'handler della programmazione ad oggetti, in sostanza un identificativo) e che nel nostro caso va a finire in fd.
Dopo di ciò viene impostato il flag per fare in modo che l'interfaccia venga aperta in modalità promiscua (vedi la linea di codice indicata nel listato) e infine, se tutto è andato bene, viene restituito il file descriptor del socket a main.
Per il momento ci fermiamo qui: nel prossimo numero continueremo la nostra analisi del sorgente di linsniff.c con le altre funzioni e vedremo come compilarlo e usarlo, e sorattutto come evitare che qualcuno lo utilizzi contro di noi.

Roberto "dec0der" Enea